أثر الإفصاح عن مخاطر الأمن السيبرانى فى التقارير المالية على أسعار الأسهم وأحجام التداول

دراسة مقارنة فى قطاع تكنولوجيا المعلومات

دكتور طارق عبدالعظيم يوسف الرشيدى
أستاذ مساعد المحاسبة
كلية التجارة – جامعة دمياط

دكتورة داليا عادل عباس السيد
أستاذ مساعد المحاسبة
كلية التجارة – جامعة دمياط

المستخلص

يهدف هذا البحث إلى التعرف على طبيعة الإفصاح عن مخاطر الأمن **السيبرانى فى التقارير المالية وعن برنامج إدارة مخاطر الأمن السيبرانى** فى الشركات المصرية المسجلة فى قطاع تكنولوجيا المعلومات حيث أنه أكثر القطاعات المعرضة للتهديدات والحوادث السيبرانية وفقا لما ورد بالإستراتيجية الوطنية المصرية للأمن السيبرانى (٢٠١٧-٢٠٢١) ومقارنة ذلك بطبيعة الإفصاح عن مخاطر الأمن السيبرانى وأثره على أسعار الأسهم وأحجام التداول فى الشركات الأمريكية وخاصة التى شهدت أخطر الهجمات السيبرانية مؤخرا والمسجلة فى هيئة البورصة الأمريكية بعد إصدار إرشادات خاصة بالإفصاح عن هذه المخاطر وبرنامج إدارتها فى عام ٢٠١٨ وإصدار المعهد الأمريكى للمحاسبين القانونيين إطارًا عامًا للتقرير عن مخاطر الأمن السيبرانى فى عام ٢٠١٧.

وقد أظهرت الدراسة ضعف الإفصاح عن مخاطر الأمن السيبرانى وبرامج إدارة مخاطره فى الشركات المصرية المسجلة فى قطاع تكنولوجيا المعلومات مقارنة بالشركات الأمريكية وما يحمله ذلك من آثار سلبية على أسعار الأسهم وأحجام التداول؛ وبناء على ذلك تم رفض فرض الدراسة **الأول** بأنه لا يوجد تأثير جوهرى للإفصاح عن مخاطر الأمن السيبرانى على أسعار الأسهم، ورفض فرض الدراسة **الثانى** بأنه يوجد تأثير

جوهرى للإفصاح عن الهجمات السيبرانية على زيادة أحجام التداول، وقبول فرض الدراسة **الثالث الخاص** بوجود فرق جوهرى فى طبيعة الإفصاح بين الشركات المصرية المسجلة فى قطاع تكنولوجيا المعلومات والشركات الأمريكية المسجلة فى هذا القطاع.

وتوصى الدراسة بسرعة إصدار كل من البورصة المصرية والهيئة العامة للرقابة المالية والبنك المركزى المصرى الضوابط والإرشادات اللازمة لدعم الإفصاح عن أنشطة الأمن السيبرانى وأية حوادث تتعرض لها أو مخاطر تهددها وبرامج إدارة مخاطر الأمن السيبرانى لديها، وأن يتولى مجلس معايير المحاسبة الدولية IASB إصدار معيار ينظم جوانب الإفصاح المحاسبى عن أنشطة ومخاطر الأمن السيبرانى وبرنامج إدارة مخاطر الأمن السيبرانى للشركات.

الكلمات الإفتتاحية: الهجمات السيبرانية Cyberattacks– الأمن السيبرانى Cybersecurity – الإفصاح عن مخاطر الأمن الإلكترونى Cybersecurity risk disclosure، إدارة المخاطر السيبرانية Cyber risk management، شركة Facebook، شركة Netflix.

The effect of Cybersecurity Disclosure in the Financial Reports on Stock Prices and Stock Volumes

A Comparative Study in the Information Technology Sector

Dr. Tarek Abdelazeem Youssef Alrashedy
Assistant Professor – Accounting

Dr. Dalia Adel Abbass Elsayed
Assistant Professor – Accounting

Faculty of Commerce – Damietta University

Abstract

This research aims at determining the nature of cybersecurity risk disclosure and the related risk management programs in thr financial reports of Eguptian Listed Companies in the Information Technology sector as it is one of the most affected sectors from cyber attaks and cyber crimes according to the Egyptian National Cybersecurity Strategy (2017-2021) and then comparing this to the nature of cybersecurity disclosure and the resulting effects on stock prices and stock volumes for the most affected American Listed Companies after the issuance of disclosure guidelines by Securities and Exchange Commision (SEC)

in 2018 and the general framework of cybersecurity risk disclosure by American Institute of Certified Public Accountants (AICPA) in 2017 .

Results show the weak cybersecurity risk disclosure in Egyptian Listed Companies in the Information Technology sector compared to their American counterparts and the resulting negative effects on the stock prices and stock volumes. So, the first research hypothesis is rejected that there is no significant effect for disclosing cybersecurity risks on stock prices, and the second research hypothesis is rejected that there is a significant positive effect of cybersecurity risk disclosure on stock volumes, and the third research hypothesis is accepted that there is a significant difference in th nature of cybersecurity risk disclosure between Listed Egyptian and American Listed companies.

Important recommendations include issuance of Cybersecurity risk disclosure guidelines by the Egyptian Stock Exchange and the General Authority of Financial Control and the Central Bank of Egypt to help companies in disclosing cybersecurity risks and their management. Also, the IASB shall issue a cybersecurity risk disclosure and management standard.

Keywords: Cyberattacks – Cybersecurity – Cybersecurity Risk Disclosur – Cybersecurity Risk Management, Netflix – Facebook.

مـقدمـة:

أدى الإعتماد المتزايد للشركات بنوعيها العام والخاص على تقنيات وشبكات الويب Web لأنظمة الإدارة المالية الخاصة بها إلى زيادة تعرضها للهجمات السيبرانية[١] (الإلكترونية) والتى تعد أحد المخاطر الرئيسية التي يجب على الشركات السيطرة عليها (Amir et al., 2018). وتتعدد أهداف هذه الهجمات فقد تكون بهدف السرقة أو تدمير الأصول المالية أو سرقة الملكية الفكرية أو غيرها من المعلومات الهامة الأخرى التى تتعلق بالشركات أو عملائها أو شركائها في العمل، واستهداف بصفة خاصة الشركات التي تعمل في صناعات البنية التحتية **الحيوية** (SEC, 2018, p.2). ومن المتوقع أن تصل تكلفة حوادث الأمن السيبرانى إلى ستة تريليون دولار بحلول ٢٠٢٥(Cybersecurity Venture 2017). وتعد تهديدات

[١] تم إستخدام مصطلح "السيبرانى" / "السيبرانية" فى الإستراتيجية الوطنية للأمن السيبرانى" وكذلك فى الدليل الإسترشادى لهيئة سوق المال السعودى وكذلك التعليمات الصادرة من البنك المركزى الأردنى فى هذا الخصوص.

الأمن السيبراني من أكثر خمسة تهديدات تواجه الإقتصاد العالمى(World Economic Forum 2017) ومن أكثر عشرة تهديدات تواجه الشركات ومستقبلها، وتفقد الأطراف المختلفة (المستثمرون، العملاء، الموردون وغيرهم) الثقة ليس فقط فى الشركة التى تتعرض لحوادث وإختراقات أمن سيبرانية (PwC, 2017) بل فى الصناعة التى تنتمى إليها الشركة بأكملها. وقد أشارت دراسة (Kelton, 2019, p.4) إلى أن العديد من الدراسات أكدت على الآثار المالية السلبية على الشركات وعلى سمعتها نتيجة الهجمات الإلكترونية التى تتعرض لها وتمتد هذه الآثار إلى الصناعة بأكملها فيما يعرف بأثر العدوى. (Wang et al., 2013; Gwebu et al., 2014; Hinz et al., 2015; Higgs et al., 2016;).

وتؤثر الهجمات السيبرانية التى يتم الإفصاح عنها على أسعار الأسهم وأحجام التداول وعوائد الأسهم مما يؤثر على أسواق رأس المال بشكل كبير؛ ويتوقف الأثر النهائى على عدة عوامل أهمها كفاءة السوق؛ ونوع خطر الأمن السيبرانى الذى يتم الإفصاح عنه، وحجم هذا الخطر؛ وحجم الشركة التى تعرضت للخطر. والملاحظ فى هذا المجال أن نتائج الدراسات قد تباينت من حيث جوهرية ونوع الأثر، فبعض الدراسات توصلت إلى عدم وجود أثار جوهرية للإفصاح عن مخاطر الأمن السيبرانى على أسعار الأسهم وأحجام التداول، وبعض الدراسات توصلت إلى وجود آثار سلبية على أسعار الأسهم وآثار إيجابية على أحجام التداول نتيجة إتجاه المستثمرين للبيع.

وأعلن التقرير السنوى الصادر عن شركة سيسكو[٢] CISCO فى ٢٠١٧ أن ٢٠٪ من الشركات التي تم اختراقها عانت من خسائر كبيرة في الإيرادات وقاعدة العملاء وفرص العمل، وأنفقت معظم الشركات التي تم اختراقها ملايين الدولارات على تحسين الحلول الأمنية وتوسيع نطاق الإجراءات الأمنية بعد الهجمات الإلكترونية (CISCO, 2017). كما أن أسهم الشركات التى تتعرض للهجمات الإلكترونية تنخفض قيمتها بنسبة ١,٨% فى المتوسط وبشكل دائم. ومع ذلك فإن الشركات لا تقدم على الإستثمار في تكنولوجيا الأمن السيبرانى إلا من خلال التنظيمات الملزمة (Haapamäki, 2019, p.4).

[٢] شركة Cisco هى شركة عالمية رائدة فى مجال تقنية المعلومات والشبكات.

وإستجابة لشكاوى الأطراف المعنية من عدم وجود معلومات كافية وفي الوقت المناسب عن مخاطر الأمن السيبرانى التى تتعرض لها الشركات وجهود الشركات فى إدارة هذه المخاطر زاد إهتمام المجالس التنظيمية والمجالس المعنية بإصدار الإرشادات المحاسبية لدعم إفصاح الشركات عن مخاطر الأمن السيبرانى وكيفية إدارة هذه المخاطر (SEC 2011, 2018; AICPA 2017 , CMA, 2019, CBJ, 2018). فقد أصدرت هيئة البورصة الأمريكية SEC إرشادات حول الإفصاح عن عوامل خطر الأمن السيبرانى **الجوهرية** فى عام ٢٠١١ وعام ٢٠١٨، كما وضع المعهد الأمريكى للمحاسبين القانونيين AICPA إطارًا للتقرير عن مخاطر الأمن السيبرانى لإرشاد الشركات فى تعزيز إفصاحاتها المتعلقة بالأمن السيبرانى. وأصدرت هيئة سوق المال السعودى CMA دليلًا إرشاديًا للأمن السيبرانى لمؤسسات السوق المالية بهدف تحديد الضوابط المتعلقة بالأمن السيبراني لمؤسسات السوق السعودى والتي تساعد على تحسين إدارة مخاطر الأمن السيبراني من خلال تبني أفضل الممارسات العالمية وتشريعات الأمن السيبراني السعودية (هيئة سوق المال السعودية، ٢٠١٩). كما أصدر البنك المركزى الأردنى CBJ فى عام ٢٠١٨ تعليمات التكيف مع مخاطر السيبرانية كمفتاح رئيسي لرفع كفاءة القطاع المالي والمصرفي في المملكة الأردنية في مواجهة التحديات والمخاطر السيبرانية.

وكشفت دراسة استطلاعية أجرتها "كاسبرسكى" Kaspersky فى عام ٢٠١٨عن أبرز الدول العربية التى تعرضت لهجمات سيبرانية على شبكاتها وأنظمتها الصناعية ، وكانت **مصر** فى مقدمة الدول حيث جاءت فى المركز الثالث بنسبة ٥٧.٦% بعد الجزائر والمغرب. وعلى ذلك فإنه لتجنب التهديدات السيبرانية يجب تطبيق استراتيجية للأمن السيبرانى لكل شركة، بل يجب أن يتم ذلك على مستوى الدولة بأكملها بأن يكون لديها استراتيجية للأمن السيبرانى القومى؛ مع تحديد مؤسسات حكومية محددة تكون مسئولة عن وضع المعايير اللازمة لتحقيق ذلك وسرعة الاستجابة للحوادث السيبراني (World Bank, 2018). وفى مصر وضع المجلس الأعلى للأمن السيبراني، التابع لرئاسة مجلس الوزراء، برئاسة وزير الاتصالات وتكنولوجيا المعلومات فى عام ٢٠١٧ **إستراتيجية وطنية للأمن السيبرانى** فى إطار جهود الدولة لدعم الأمن القومي

وتنمية المجتمع المصري، ومع تزايد التهديدات والتحديات المستقبلية في المجال السيبرانى والمجتمع الرقمي ولرصد ومجابهة المخاطر والتهديدات المتزايدة من خلال انشاء المجلس الأعلى للأمن السيبرانى وتكنولوجيا المعلومات لتأمين البني التحتية للاتصالات والمعلومات ولتوفير البيئة الآمنة لمختلف القطاعات، تمثل فيه الأطراف المعنيين بالأمن القومي في القطاعات الحيوية والمرافق العامة، وذوي الخبرة في القطاع الخاص والجهات البحثية والتعليمية حيث يتولى المجلس وضع استراتيجية وطنية للأمن السيبرانى ولمواجهة الهجمات السيبرانية. كما يتولى الاشراف على تنفيذ تلك الاستراتيجية، مع ضرورة تحديثها تمشيا مع التطورات التقنية المتلاحقة. وقد بدأ المجلس عمله التمهيدي فى يناير ٢٠١٥ وقام رئيس مجلس الوزراء باعتماد تشكيل المكتب التنفيذي للمجلس ولجنته الفنية وتوصيف مهامه فى ٢٠١٦.

إن أهمية إدارة البيانات والتكنولوجيا ومخاطرها للشركات اليوم مماثلة لأهمية الكهرباء في القرن الماضي. وعلى الرغم من توصيات الهيئات التنظيمية ونتائج البحوث الحديثة فى الآثار السلبية المترتبة على إختراقات الأمن السيبرانى وضرورة الإفصاح عن ذلك للأطراف المعنية داخل وخارج الشركة (SEC, 2018, Amir et al., 2018; Rubin 2019; Lin et al., 2019)، لم تصدر الهيئة العامة للرقابة المالية أو البورصة المصرية أو البنك المركزى المصرى أية تعليمات لتوجيه الشركات للإفصاح عن أنشطة الأمن السيبرانى لديها والتهديدات والمخاطر التى تتعرض لها وبرنامج إدارة المخاطر لمواجهة هذه التهديدات.

ومن هنا تتضح أهمية الإجابة على **التساؤل الرئيسى** فى البحث وهو: **ما هو أثر الإفصاح عن مخاطر الأمن السيبرانى فى التقارير المالية على أسعار الأسهم وأحجام التداول فى الشركات العالمية الكبرى التى تعرضت لمخاطر الأمن السيبرانى مؤخرا؟ وما هو طبيعة الإفصاح عن أنشطة وبرامج إدارة مخاطر الأمن السيبرانى فى الشركات المصرية المسجلة فى قطاع تكنولوجيا المعلومات؟** ويتفرع عن هذا السؤال الرئيسى التساؤلات الفرعية التالية:

١- ما هى طبيعة الأمن السيبرانى فى مجال المحاسبة؟
٢- ما دور المؤسسات التنظيمية فى دعم الإفصاح عن مخاطر الأمن السيبرانى وتوصيف برامج إدارة مخاطر الأمن السيبرانى؟
٣- ما هى الآثار المختلفة المترتبة على الإفصاح عن الهجمات السيبرانية؟
٤- ما هى طبيعة الإفصاح عن مخاطر الأمن السيبرانى وإدارة مخاطره فى الشركات المصرية المسجلة فى قطاع تكنولوجيا المعلومات؟ وما هى مجالات اختلاف هذا الإفصاح عن الشركات الأمريكية المسجلة فى قطاع الإتصالات وتكنولوجيا المعلومات؟

هدف البحث:

يتمثل **الهدف الرئيسى** للبحث فى تحليل أثر الإفصاح عن مخاطر الأمن السيبرانى فى التقارير المالية على أسعار السهم وأحجام التداول فى الشركات التى تعرضت لخطر الهجمات السيبرانية مؤخرا. ويتفرع من هذا الهدف الرئيسى الأهداف الفرعية التالية:

١- تبيان طبيعة إفصاح الشركات المصرية المسجلة فى قطاع تكنولوجيا المعلومات عن أنشطة ومخاطر الأمن السيبرانى وبرامج إدارة هذه المخاطر.
٢- تحليل جهود المؤسسات التنظيمية فى دعم الإفصاح عن أنشطة ومخاطر الأمن السيبرانى وبرامج إدارة هذه المخاطر وجهود الدولة المصرية فى هذ المجال.
٣- توصيف برنامج لإدارة مخاطر الأمن السيبرانى.
٤- تحليل الآثار المختلفة المترتبة على الإفصاح عن المخاطر والهجمات السيبرانية.
٥- دراسة مقارنة لطبيعة الإفصاح فى الشركات المصرية المسجلة فى قطاع تكنولوجيا المعلومات والشركات الأمريكية العاملة فى هذا القطاع.

حدود البحث:

تم إجراء البحث من خلال الحدود التالية:

١- تم مقارنة الإفصاح فى الشركات المصرية المسجلة فى قطاع تكنولوجيا المعلومات بشركة مايكروسوفت Microsift الأمريكية وشركة فيسبوك Facebook كنموذج للمقارنة فقط.

٢- تم دراسة أثر الإفصاح عن المخاطر السيبرانية على أسعار الأسهم وأحجام التداول لشركة Netflix وشركة Facebook عامى ٢٠١٦ و٢٠١٧ على التوالى كأمثلة للشركات التى تعرضت لأخطر الهجمات السيبرانية مؤخرا دون التطرق إلى دراسة أثر باقى الهجمات السيبرانية الأخرى.

٣- تم فحص استمارة / نموذج 10-K فقط الذى يتم تقديمه سنويا للبورصة الأمريكية والذى يلخص الأداء المالى للشركة دون التطرق إلى باقى الإستمارات مثل (8-K) الذى يتم تقديمه فى حالة حدوث حدث جوهرى مثل الإفلاس أو (10-Q) وهو تقرير ربع سنوى عن الأداء المالى للشركة.

٤- تم تحليل طبيعة الإفصاح فى الشركات المصرية من خلال فحص أحدث القوائم والتقارير المالية المنشورة لهذه الشركات والمسجلة فى قطاع تكنولوجيا المعلومات.

خطة البحث:

تم تقسيم البحث من خلال أربعة عناصر كما يلى:

أولا: الدراسات السابقة.

ثانيا: أثر الإفصاح عن مخاطر الأمن السيبرانى وأسعار السهم وأحجام التداول.

ثالثا: دور المؤسسات التنظيمية فى الإفصاح عن إدارة مخاطر الأمن السيبرانى ودور المحاسبة فى برنامج إدارة المخاطر السيبرانية.

رابعا: الدراسة التطبيقية واختبار الفروض.

أولا: الدراسات السابقة.

قام (Haapamäki, 2019, p.9) بمراجعة الأبحاث المحاسبية المنشورة فى الفترة ما بين عام ٢٠٠٠ إلى عام ٢٠١٨ المنشورة فى الدوريات العلمية المرموقة ذات التأثير المرتفع من خلال البحث فى سكوباس Scopus وجوجل سكولرز Google Scholars والمتعلقة بالأمن السيبرانى ووجد ٣٩ دراسة صنفها فى **خمس مجموعات: الأولى** تتعلق بمشاركة المعلومات والأمن السيبرانى وعددها ٤ أبحاث والمجموعة **الثانية** تتعلق بالإستثمارات فى الأمن السيبرانى وعددها ٨ أبحاث والمجموعة **الثالثة** تتعلق بالرقابة والمراجعة الداخلية والأمن السيبرانى وعددها ١٣ بحث والمجموعة **الرابعة** تتعلق بالإفصاح عن أنشطة الأمن السيبرانى وعددها ٥ أبحاث والمجموعة **الخامسة** تتعلق بالتهديدات والإختراقات السيبرانية وعددها ٩ أبحاث، وتشير هذه النتائج إلى النقص فى عدد الأبحاث التى تناولت موضوع الإفصاح عن أنشطة الأمن السيبرانى بشكل عام وندرة الدراسات التى تناولت الإفصاح عن إدارة مخاطر الأمن السيبرانى فى مصر بشكل خاص.

وقام (Gordon et al.2006) بإجراء دراسة تطبيقية عن تأثير قانون سوربينز أوكسلي SOX2002 على الإفصاح الإختيارى للشركات عن أنشطة الأمن السيبرانى. وتوصلت الدراسة إلى أن تطبيق قانون SOX2002 كان له تأثير إيجابي على الإفصاح الإختيارى عن أنشطة الأمن السيبرانى حيث زاد الإفصاح الإختيارى عن أنشطة الأمن السيبرانى بأكثر من ١٠٠% منذ تطبيق هذا القانون بالمقارنة بالعامين السابقين لتطبيق القانون على الرغم من أن القانون لم يشر بوضوح إلى موضوع الأمن السيبرانى. ويمكن التعليق على ذلك بأنه يجب وجود قانون يلزم الشركات المصرية المسجلة بسوق الأوراق المالية بالإفصاح عن أنشطة الأمن السيبرانى والإفصاح عن أية هجمات سيبرانية تتعرض لها ونظام إدارة مخاطر الأمن السيبرانى.

وفى ذات الإتجاه تناولت دراسة (Gordon et al., 2010) فحص الإفصاحات الإختيارية المتعلقة بالأمن السيبرانى من خلال دراسة تطبيقية بإستخدام أسلوب الإنحدار المتعدد، وتوصلت الدراسة إلى أن الإفصاحات الإختيارية فى التقارير السنوية تسمح للشركات بإعطاء مؤشرات للسوق بأن الشركة نشطة فى منع وإكتشاف وتصحيح الإنتهاكات السيبرانية. وبالتالى فإن إختيار الشركة بأن تقوم بالإفصاح السيبرانى عن البنود التى تتعلق بالأمن السيبرانى من عدمه يعتبر إختيارًا استراتيجيًا وأن عدد الشركات التى تقوم بالإفصاح

السيبرانى عن المعلومات التى تتعلق بأمن المعلومات فى ازدياد، بالإضافة إلى تأثيره الإيجابى القوى على سعر السهم وعلى القيمة السوقية للشركة. وأن الشركات التى لديها مقاييس استباقية تتعلق بالأمن السيبرانى لها التأثير الأقوى على الإطلاق على سوق الشركة.(Gordon et al., 2010, p. 590).

وعلى النقيض من ذلك فحصت دراسة (Wang et al., 2013) الإرتباط بين الإفصاح وإدراك مخاطر الأمن السيبرانى وتوصلت الدراسة إلى أن الشركات غالبا ما تقوم بالإفصاح عن عوامل خطر أمن المعلومات فى التقارير الرسمية public filings وأن معلومات الأمن الإلكترونى الداخلية التى يتم الإفصاح عنها قد تكون سلبية أو إيجابية. وتم تقييم كيفية إرتباط طبيعة عوامل مخاطر الأمان التى يتم الإفصاح عنها والتى يمكن أن تمثل المعلومات الداخلية للشركة عن أمن المعلومات بالإعلان عن إختراقات فى وسائل الإعلام فى المستقبل، وذلك من خلال نموذج شجرة القرارات حيث تم تصنيف حدوث الإختراقات على أساس المحتويات النصية لعوامل مخاطر الأمان المفصح عنها. وكانت نسبة دقة النموذج فى ربط خصائص الإفصاح بالإعلان عن الإنتهاكات فى وسائل الإعلام ٧٧ %. كما استخدمت تقنيات استخراج النص text-mining techniques فى تفسير النتائج وتم التوصل من خلالها إلى أن عوامل خطر الأمان التي تم الإفصاح عنها والتي تتضمن موضوعات تخفيف المخاطر risk mitigation themes أقل ارتباطًا بالإعلان عن الاختراق السيبرانى في المستقبل، مما يشير إلى أن رد فعل السوق بعد الإعلان عن الإختراقات السيبرانية تتوقف على طبيعة الإفصاح السابق له. وبالتالى فإن المحتوى النصى لعوامل مخاطر الأمان يعتبر مؤشرا للإختراقات المستقبلية التى يتم التقرير عنها. لذلك فإن الشركات التى تفصح عن معلومات خاصة بتخفيض المخاطر تكون أقل إحتمالا لتعرضها لحوادث خاصة بالأمان. ولذلك يكون لدى هذه الشركات الحافز للإفصاح عن موقفهم من أمن المعلومات بصدق.

وتناولت دراسة (Li et al. 2018) العلاقة بين الإفصاح عن مخاطر الأمان السيبرانى وحدوث جرائم الأمن السيبرانى فى المستقبل من خلال دراسة تطبيقية باستخدام تحليل الانحدار. وقد تم التركيز على مقياسين هما: وجود إفصاح عن مخاطر الأمن السيبرانى؛ وحجم legnth الإفصاح عن مخاطر الأمن

السيبرانى. وقد توصلت الدراسة إلى أن وجود عوامل المخاطر فى فترة ما قبل وجود الإرشادات وحجم عوامل المخاطر ترتبط بوقوع جرائم الأمن السيبرانى التى يتم التقرير عنها فى المستقبل. ولكن الإرتباط بين وجود الإفصاح عن مخاطر الأمن الإلكترونى وجرائم الأمن السيبرانى التى تم الإعلان عنها بعد ذلك أصبح غير جوهرى بعد إصدار إرشادات الإفصاح الخاصة بالأمن السيبرانى التى أصدرتها هيئة البورصة الأمريكية. ولكن يجب توخى الحذر عند تفسير النتائج حيث أشارت الدراسة إلى أن هذه الإرشادات قد تشجع الشركات عن غير قصد الكشف عن مخاطر الأمن السيبرانى بغض النظر عن مستوى المخاطر.

وناقشت دراسة (Ettredge et al., 2018) العلاقة بين إفصاح الشركات عن وجود أسرار تجارية فى نماذج 10-K والسرقات السيبرانية لبيانات الشركات والتى تعرف بإختراقات الأمن السيبرانى من خلال دراسة تطبيقية باستخدام تحليل الانحدار. وتوصلت الدراسة إلى أن الشركات التي أشارت إلى وجود أسرار تجارية لديها احتمال أكبر بكثير من أن يتم اختراقها فى المستقبل مقارنة بالشركات التي لا تفعل ذلك. وكانت النتائج أقوى بالنسبة للشركات الأحدث والشركات التي لديها عدد أقل من العاملين والشركات العاملة في الصناعات الأقل تركيزا less concentrated industires.

وبالتالى يتضح أهمية إصدار إرشادات الإفصاح الخاصة بالأمن السيبرانى لدعم الإفصاح عن مخاطر الأمن السيبرانى لتأثيره الإيجابى على سعر السهم وعلى القيمة السوقية للشركة وخفض جرائم وحوادث الأمن السيبرانى.

ثانيا: أثر الإفصاح عن مخاطر الأمن السيبرانى على أسعار السهم وأحجام التداول.

يؤثر الإفصاح عن الهجمات والإختراقات السيبرانية على أسعار الأسهم وأحجام التداول حيث تمثل التغيرات الكبيرة والسلبية مؤشرا هاما لرد فعل المستثمرين نتيجة ذلك الإفصاح والذى يؤثر على قيمة الشركة. فعلى الرغم من صعوبة قياس التكلفة الحقيقية للأضرار التي تلحق بالشركات في كثير من الأحيان إلا أن هذه التغيرات تمثل طريقة فعالة لتقييم الأثر الاقتصادي الفوري للتهديدات والهجمات السيبرانية. إن كفاءة

السوق تعني أن المعلومات والأرباح والتدفقات النقدية المستقبلية التى تفصح عنها الشركة تنعكس على الفور على أسعار الأسهم وإتجاه التداول، وبالتالى فإن أثر الإفصاح عن الهجمات السيبرانية يمكن قياسه من خلال حجم التغيرات السلبية فى أسعار الأسهم وأحجام وإتجاه التداول خاصة بعد الإعلان عن الهجمات السيبرانية مباشرة (Bianchi et al., 2019, p. 3).

وقد ركز(Bianchi et al., 2019, p. 1) على دراسة أثر الإفصاح عن التهديدات والهجمات السيبرانية على الشركات وسوق رأس المال فى الأجل القصير والأجل الطويل وتوصل إلى أنه عندما تقوم الشركة بالإفصاح عن هجوم سيبرانى لأول مرة فإنه توجد آثار على المدى القصير وآثار على المدى الطويل. بالنسبة للآثار على المدى القصير فإنها تتمثل فى انخفاض العوائد اليومية غير العادية وزيادة حجم التداول بسبب ضغط البيع وتتدهور السيولة. وعلى المدى الطويل –حتى خمس سنوات– تتأثر سياسات الشركات نتيجة الأضرار الكبيرة على سمعة الشركات. وأشارت هذه الدراسة إلى وجود عدد قليل من الدراسات التى تناولت أثر الإفصاح عن الهجمات السيبرانية على أسعار الأسهم فى الأجل القصير والتى توصلت إلى إنخفاضها بدرجة كبيرة (Goel et al. 2009, Spanos et al., 2016).

وأكد(Richardson, 2019, p.4)على أن نتائج الدراسات السابقة فيما يتعلق بأثر الإفصاح عن اختراقات الأمن السيبراني على سلوك أسعار الأسهم متضاربة وذلك يرجع إلى سببين أساسيين.**الأول** هو اختلاف نوع المعلومات التي يتم الحصول عليها من الهجمات السيبرانية فإذا كانت على سبيل المثال إختراق السجلات الخاصة بالعملاء كما في حالة شركة Equifax فإن ذلك سيفقد العملاء ثقتهم فى الشركة،ولكن إذا كانت هجمات البرمجيات الخبيثة attacks malware لشركات تصنيع فإن الأثر الأكثر احتمالا هو إنخفاض التدفقات النقدية وليس فقد ثقة العملاء فقط بسبب طبيعة المنتجات التى تقدمها(Berr et al, 2017) . وقد تستغرق تأثيرات الأنواع المختلفة من الهجمات وقتًا طويلاً حتى تحدث بالنسبة للشركات التي تعتمد أكثر على رأس المال الفكرى كميزة تنافسية في السوق. والسبب **الثانى** أنه على الرغم من أن العديد من الهجمات السيبرانية تحدث بدون معرفة الشركة وهو ما يؤكد حالة عدم التأكد المتعلقة بنقاط الضعف لها فإنه قد لا

يكون لدى الشركات التي تكتشف الحوادث السيبرانية حافزًا للإفصاح عن التفاصيل الكاملة للهجوم السيبرانى كما حدث في حالة Yahoo (Collins et al., 2017) حيث أفصحت الشركة فى أواخر عام ٢٠١٦ أنها تعرضت لحادثي إختراق بيانات أكثر من ٥٠٠ مليون مستخدم وبليون مستخدم على التوالى فى ٢٠١٣. وبمجرد الإعلان عن ذلك إنخفض سعر سهم Yahoo بمعدل ٤,٤% فى شهور قليلة وبلغت قيمة الإنخفاض الإجمالية للقيمة الإجمالية ١,٧ بليون دولار (Spanos et al., 2016). بل إن ذلك أدى إلى إنخفاض سعر صفقة إتمام إستحواذ شركة Verizon على شركة Yahoo من ٤,٨٣ بليون دولار إلى ٤,٤ بليون دولار أى بمعدل ٧,٢٥%. وبعد ذلك فى عام ٢٠١٧ تبين أن الحادث أثر على ٣ بليون حساب وليس بليون حساب.

كما أكدت نفس الدراسة على أن (Spanos et al., 2016) قاموا بمراجعة ٤٥ دراسة وتوصلوا إلى أن حوالى ١١ دراسة تقريبا منها لم تتوصل إلى وجود علاقة إحصائية قوية بين الإفصاح عن الهجمات السيبرانية وأسعار الأسهم، وحتى لو حدث إنخفاض لأسعار الأسهم فإنها سريعا ما تعود للإرتفاع مرة أخرى خلال يومين من الإفصاح عن الحوادث السيبرانية (Cavusoglu et al., 2014). وأثبتت دراسة Lange et al., 2017) أن العائد على السهم ينخفض فى الثلاثة أيام التالية للإفصاح عن الهجمات السيبرانية بنسبة ١, ١٣% بينما يعاود الإرتفاع فى اليوم الرابع عشر من الإفصاح. وأكدت دراسة (Kammoun et al., 2019) على هذه النتائج أيضا.

وتوصلت دراسة (Rosati et al., 2017, p.4) إلى أن الإفصاح عن الهجمات السيبرانية له تأثير إيجابى فى الأجل القصير على حجم التداول نظرا للإتجاه للبيع لتجنب الخسائر المحتملة. ويكون حجم الأثر أكبر فى الهجمات السيبرانية الكبيرة وللشركات الكبرى.

فروض الدراسة:

فى ضوء نتائج الدراسات السابقة التى تم عرضها وتحليلها فإنه يمكن إشتقاق فرضى الدراسة الأول والثانى كما يلى:

الفرض الأول: " لا يوجد تأثير جوهرى للإفصاح عن مخاطر الأمن السيبرانى على **أسعار الأسهم** ".

الفرض الثانى:" يوجد تأثير جوهري للإفصاح عن مخاطر الأمن السيبرانى على زيادة **حجم التداول** للأسهم".

ثالثا: دور المؤسسات التنظيمية فى الإفصاح عن إدارة مخاطر الأمن السيبرانى ودور المحاسبة فى برنامج إدارة المخاطر السيبرانية.

تمت جهود من جانب كل من المعهد الأمريكى للمحاسبين المعتمدين؛ وهيئة البورصة الأمريكية؛ وجهود مصرية فى دعم الإفصاح عن مخاطر الأمن السيبرانى؛ والاهتمام بدور المحاسبة فى برنامج إدارة هذه المخاطر المتزايدة.

I. جهود المؤسسات التنظيمية فى الإفصاح عن إدارة مخاطر الأمن السيبرانى.

١- دور المعهد الأمريكى للمحاسبين المعتمدين.

وضع المعهد الأمريكى للمحاسبين القانونيين إطارًا للتقرير عن إدارة مخاطر الأمن السيبرانى فى عام ٢٠١٧ لإرشاد الشركات ودعمهم فى الإفصاح عن المخاطر السيبرانية. ويتكون الإطار من ثلاثة عناصر رئيسية وهى: وصف الإدارة لبرنامج إدارة مخاطر الأمن السيبراني للشركة، وتأكيدات الإدارة فيما يتعلق بفعالية ضوابط الأمن السيبراني، ورأي المراجع الخارجى في إفصاحات الإدارة وفعالية ضوابط الشركة (مثل تقرير ضوابط النظام للأمن السيبراني).

وقد تم وصف برنامج إدارة مخاطر الأمن السيبرانى من خلال العناصر التالية (AICPA, 2017):

١- طبيعة أعمال الشركة وعملياتها وتشمل المنتجات أو الخدمات الرئيسية التي تبيعها أو تقدمها والطرق التي يتم بها توزيعها.

٢- الأنواع الرئيسية من المعلومات الهامة التى يتم يتم إنشاؤها أو تجميعها أو إرسالها أو استخدامها أو تخزينها بواسطة المنشأة.

٣- أهداف برنامج إدارة مخاطر الأمن السيبرانى وتشمل الأهداف الرئيسية لبرنامج إدارة مخاطر الأمن السيبراني (أهداف الأمن السيبراني) المتعلقة بتوافر البيانات وسريتها وسلامتها وسلامة المعالجة، بالإضافة إلى عملية إنشاء والحفاظ على والموافقة على أهداف الأمن السيبراني لدعم تحقيق أهداف المنشأة.

٤- العوامل التي لها تأثير كبير على المخاطر الحتمية للأمن السيبرانى وتشمل **العوامل التي لها تأثير كبير على مخاطر الأمن السيبراني للشركة** ويشمل: خصائص التكنولوجيا وأنواع الاتصال واستخدام مقدمي الخدمات وقنوات التسليم التي تستخدمها المنشأة، الخصائص التنظيمية وخصائص المستخدم، والتغييرات البيئية والتكنولوجية والتنظيمية وغيرها خلال فترة وصف المنشأة لبرنامج إدارة مخاطر الأمن السيبرانى، وبالإضافة إلى ذلك فإنه بالنسبة للحوادث الأمنية التي تم تحديدها خلال فترة الاثني عشر شهرًا التي سبقت تاريخ إنتهاء الفترة لوصف الإدارة لبرنامج إدارة المخاطر ونتج عنها انخفاض كبير في تحقيق المنشأة لأهداف الأمن السيبراني فإنه يجب الإفصاح عما يلي: طبيعة الحادث وتوقيت حدوثه ومدى والتأثير المختلفة لهذه الحوادث وطرق معالجتها.

٥- هيكل **حوكمة** إدارة المخاطر ويشمل عملية إنشاء وصيانة والتقرير عن النزاهة والقيم الأخلاقية لدعم عمل برنامج إدارة مخاطر الأمن السيبراني، بالإضافة إلى عملية إشراف مجلس الإدارة على برنامج إدارة مخاطر الأمن السيبراني للشركة، وكذلك أسس المساءلة وخطوط التقرير في مجال الأمن السيبراني، بالإضافة إلى العملية المستخدمة لتوظيف وتطوير الأفراد والمتعاقدين الكفء ومحاسبة هؤلاء الأفراد عن مسؤولياتهم المتعلقة بالأمن السيبراني.

٦- عملية **إدارة مخاطر الأمن السيبرانى** وتشمل عملية تحديد المخاطر السيبرانية والتغييرات البيئية والتكنولوجية والتنظيمية التى يمكن أن يكون لها تأثير جوهرى على برنامج إدارة مخاطر الأمن السيبرانى للمنشأة وتقدير المخاطر المتعلقة بتحقيق المنشأة لأهداف الأمن السيبرانى، وكذلك عملية تحديد وتقييم وإدارة المخاطر المرتبطة بالموردين وشركاء الأعمال.

٧- قنوات **إتصال** الأمن السيبراني وجودة معلومات الأمن السيبراني وتشمل عملية توصيل المعلومات للأطراف الداخلية المتعلقة الأمن السيبراني واللازمة لدعم عمل برنامج إدارة مخاطر الأمن السيبراني للمنشأة وتشمل أهداف ومسئوليات الأمن السيبراني وحدود توصيل حوادث الأمن التي تتم مراقبتها والتحقيق فيها والتي تتطلب استجابة أو علاج أو كليهما، وكذلك عملية توصيل المعلومات التي تؤثر على أداء برنامج إدارة مخاطر الأمن السيبراني للمنشأة مع الأطراف الخارجية.

٨- رقابة برنامج **إدارة مخاطر** الأمن السيبرانية وتشمل عملية إجراء تقييمات مستمرة ودورية للفعالية التشغيلية لأنشطة الرقابة الرئيسية والمكونات الأخرى للرقابة الداخلية المتعلقة بالأمن السيبراني، بالإضافة إلى العملية المستخدمة فى تقييم وتوصيل التهديدات الأمنية ونقاط الضعف وأوجه القصور فى الضوابط الرقابية في الوقت المناسب للأطراف المسؤولة عن اتخاذ الإجراءات التصحيحية وتشمل الإدارة العليا ومجلس الإدارة.

٩- أنشطة **مراقبة** الأمن السيبرانى وتشمل عملية تطوير استجابة المخاطر المتوقعة بما في ذلك تصميم وتنفيذ عمليات الرقابة، وكذلك ملخص للبنية التحتية لتكنولوجيا المعلومات في المنشأة والخصائص المعمارية لشبكتها، بالإضافة إلى السياسات والعمليات الأمنية الرئيسية التى تم تنفيذها وتشغيلها لمعالجة مخاطر الأمن السيبراني للمنشأة ويشمل ذلك المخاطر التي تتناول ما يلي: منع الحوادث الأمنية المتعمدة وغير المقصودة والكشف عن وتحديد الحوادث الأمنية وتطوير طرق الاستجابة لتلك الحوادث وأنشطة للتخفيف من الحوادث الأمنية والتعافي منها وإدارة القدرة التشغيلية لتوفير العمليات المستمرة أثناء الحوادث الأمنية والتشغيلية والبيئية والكشف عن الحوادث البيئية وتخفيفها والتعافى السريع منها واستخدام إجراءات تتعلق بضمان وجود نسخ احتياطية لدعم توفر النظام وتحديد المعلومات السرية عند تلقيها أو إنشائها، وتحديد فترة الاحتفاظ بهذه المعلومات لفترة محددة، والتخلص من المعلومات في نهاية الفترة، وكذلك منع الحوادث الأمنية المتعمدة وغير المتعمدة، واكتشاف وتحديد الحوادث الأمنية وتطوير الإستجابة لتلك الحوادث.

٢- دور لجنة البورصة الأمريكية Securities and Exchange Commission (SEC) (SEC, 2018):

أصدرت هيئة البورصة الأمريكية فى ٢٦ فبراير ٢٠١٨ دليلا يتضمن إرشادات للشركات الأمريكية المسجلة تتعلق **بمتطلبات الإفصاح عن الأمن السيبرانى** ويتكون الدليل من قسمين، **القسم الأول** المقدمة وتتكون من ثلاثة عناصر: **العنصر الأول** طبيعة الأمن السيبرانى حيث تناول تعريف الأمن السيبرانى ومخاطره على المستثمرين والشركات وأسواق المال وطرق حدوث الحوادث السيبرانية وأهدافها والآثار السلبية لحدوثها وأهمية الإفصاح عن ذلك للأطراف المعنية والمستفيدة وأثر ذلك على الشركة وعملياتها وموقفها المالى مع التحذير من أهمية عدم إجراء أية تعاملات داخلية على الأسهم بواسطة الأطراف ذات العلاقة بالشركة فى حالة حدوث أية حوادث سيبرانية وقبل الإفصاح عن ذلك لجميع الأطراف.

وتناول **العنصر الثانى** دليل وإرشادات الإفصاح عن المن السيبرانى والتى بدأت فى أكتوبر ٢٠١١ مع التأكيد على أنه بالرغم من أنه لم يتم الإشارة صراحة إلى متطلبات إفصاح عن مخاطر وحوادث الأمن السيبرانى التى تتعرض لها الشركة فى هذا الدليل إلا أنه قد تكون الشركات ملزمة بالإفصاح عن هذه المخاطر والحوادث. وهذا ما حدث بالفعل حيث إزداد إفصاح الشركات عن الأمن السيبرانى كعوامل مخاطرة.

وتناول **العنصر الثالث** الغرض من إصدار عام ٢٠١٨ وهو التوسع فى متطلبات الإفصاح الصادرة فى ٢٠١١ بإضافة بندين أساسيين وهما: الأول يتعلق بأهمية وجود سياسات وإجراءات بالشركات تتعلق بحوادث ومخاطر الأمن السيبرانى حيث يجب على الشركات إنشاء إجراءات ورقابات إفصاح فعالة تساعدها أن تقدم معلومات دقيقة وفى الوقت المناسب عن الأحداث الجوهرية التى تتعلق بالأمن السيبرانى. والثانى يتعلق بمنع قيام الأطراف ذات العلاقة بتعاملات داخلية فى حالة حدوث حوادث ومخاطر تتعلق بالأمن السيبرانى.

وتكون **القسم الثانى** المتعلق بإرشادات الإصدار من عنصرين، **العنصر الأول:** مراجعة للقواعد التى تتعلق بالإفصاح عن مشكلات الأمن السيبرانى ويتناول الأهمية النسبية وعوامل الخطر والموقف المالى ونتائج

العمليات ووصف العمليات والإجراءات القانونية وإفصاحات القوائم المالية ومراقبة المجلس للمخاطر، **والعنصر الثانى:** السياسات والإجراءات ويتكون من إجراءات ورقابات الإفصاح والتعاملات الداخلية والتنظيمات والإفصاحات الإنتقائية وفيما يلى شرحا مختصرا لهذه العناصر.

وبالنسبة **للعنصر الأول** المتعلق بمراجعة القواعد التى تتعلق بالإفصاح عن مشكلات الأمن السيبرانى فإنه يشمل:

أولا: الأهمية النسبية.

حيث يجب على الشركات النظر في مدى أهمية مخاطر الأمن السيبراني وحوادثه عند إعداد التقارير الدورية السنوية (k–10) والربع سنوية (Q–10). ويجب أن تفصح الشركات عن المعلومات المتعلقة بمخاطر وحوادث الأمن السيبراني الجوهرية فى التقارير الدورية فى الوقت المناسب وبصفة مستمرة بشكل كاف. ولكن فى حال وجود معلومات جوهرية تتعلق بالأمن السيبراني فإنه يجب استخدام النموذج (k–8) أو النموذج (k–6) للإفصاح عنها فورا حيث يقلل ذلك من خطر الإفصاح الانتقائى، وكذلك خطر حدوث التداول على أساس المعلومات غير العامة الجوهرية.

ويعتمد تحديد جوهرية مخاطر الأمن أو الحوادث السيبرانية على طبيعتها ومداها وحجمها المحتمل خاصة فيما يتعلق بصلتها بأي معلومات معرضة للخطر أو الأعمال التجارية ونطاق عمليات الشركة. وتعتمد مخاطر وحوادث الأمن السيبراني أيضًا على مدى الضرر الذي قد تسببه مثل هذه الحوادث ويشمل ذلك الضرر بسمعة الشركة وأدائها المالي وعلاقاتها مع العملاء والموردين وكذلك إمكانية التقاضي. ولا يعنى ذلك أن تقوم الشركة بالإفصاح المفصل بما يؤثر بالسلب على جهود الأمن السيبراني الخاصة بها مما يسهل من اختراق الحماية الأمنية للشركة. ولكن ما يجب الإفصاح عنه هو مخاطر وحوادث الأمن السيبراني التي تعتبر هامة للمستثمرين وما يترتب عليها من آثار مالية أو قانونية أو إضرار بسمعة الشركة. واتخاذ خطوات

لمنع أعضاء مجلس الإدارة والموظفين والأطراف ذات العلاقة من تداول أوراقها المالية حتى يتم إعلام المستثمرين بشكل مناسب بالحادث أو المخاطر الملرتبطة به .

وقد تحتاج الشركة إلى بعض الوقت أثناء إجراء التحقيقات الداخلية أو الخارجية الخاصة بوقائع الأمن السيبرانى وهذا لا يعنى تجنب الإفصاح عنها حتى يتم الإنتهاء من التحقيقات والتى غالبا ما تستغرق فترة زمنية طويلة. ولذلك قد تكتشف الشركة أثناء التحقيقات أنه يجب تصحيح إفصاحات سابقة عن حوادث الأمن السيبرانى لأنها كانت غير صحيحة أو أنها بحاجة إلى تحديثها، وفى هذه الحالة يجب أن تقوم بالإفصاح عن التصحيح والتحديث خاصة لو كان ذلك جوهريا. ولا يمكن تقديم متطلبات ثابتة لإفصاح الشركات عن حوادث ومخاطر الأمن السيبرانى حيث يختلف ذلك من شركة لأخرى حسب حادثة الأمن السيبرانى التى تعرضت لها ولكن ذلك لا يعنى أن تكون عبارات الإفصاح عامة وأن تكون محددة ومفيدة للمستثمرين وبالتالى فإنه يجب أن تقوم الشركة بالإفصاح عن المعلومات الملائمة والجوهرية بحيث تتوفر بها خاصيتى الإكتمال والمقارنة بين الشركات.

ثانيا: عوامل الخطر:

يجب على الشركة الإفصاح عن المخاطر المرتبطة بالأمن السيبرانى وحوادثه بما فى ذلك المخاطر التى تنشأ عند الإستحواذ. ومن المفيد أن تقوم الشركات أن تأخذ فى الإعتبار العوامل التالية عند تقييم الإفصاح عن عوامل مخاطرة الأمن السيبرانى:

- حدوث حوادث سابقة للأمن السيبرانى وحدتها ومدى تكرارها.
- إحتمال حدوث والحجم المحتمل لحوادث الأمن السيبرانى.
- مدى كفاية الإجراءات المانعة لخفض مخاطر الحوادث السيبرانية والتكاليف المرتبطة بذلك.
- خصائص عمليات الشركة التى تزيد من حدوث المخاطر السيبرانية الجوهرية بما فى ذلك خصائص الصناعة.

-التكاليف المرتبطة بحماية الأمن السيبرانى مثل التأمين على حوادث الأمن السيبرانى.

-الإضرار بسمعة الشركة.

-القوانين والتنظيمات التى تتعلق بمتطلبات الأمن السيبرانى وتكاليف ذلك.

-تكاليف التحقيقات التنظيمية والقضائية وحل مشكلات حوادث الأمن السيبرانى.

يجب على الشركات الإفصاح عن حوادث الأمن السيبراني السابقة أو التى مازالت موجودة وعواقبها وأنواع حوادث الأمن السيبراني المحتملة التى تشكل مخاطر خاصة على أعمال الشركة وعملياتها وكذلك الحوادث السابقة التي تتضمن موردين أو عملاء أو منافسين وغيرهم من الملائم الإفصاح عنها فى سياق الإفصاح عن المخاطر السيبرانية بفعالية للمستثمرين.

ثالثا: الموقف المالى ونتائج العمليات

يجب على الشركة الإفصاح عن أية أحداث من المحتمل أن يكون لها تأثيرا جوهريا على نتائج العمليات والموقف المالى بما فى ذلك تكلفة المجهودات وأنشطة الدعم المستمرة الخاصة للأمن السيبرانى والتكاليف والنتائج الأخرى للحوادث السيبرانية المحتملة. وكذلك التكاليف العديدة المرتبطة بمشكلات الأمن السيبرانى مثل خسارة حقوق الملكية الفكرية وفقد الموقف التنافسى وتكاليف الإجراءات المانعة لحدوثها والتأمين والتحقيقات التنظيمية والقضائية والإعداد للتشريعات الحالية أو المقترحة.

رابعا: وصف طبيعة النشاط

يجب على الشركة الإفصاح عن الحوادث أو المخاطر السيبرانية التى من شأنها التاثير الجوهرى على المنتجات أوالخدمات أو العلاقات مع العملاء أوالموردين أوالموقف التنافسي.

خامسا: الإجراءات القانونية:

يجب على الشركات الإفصاح عن المعلومات المتعلقة بالقضايا الجوهرية المعلقة المتعلقة بقضايا الأمن السيبرانى سواء بالنسبة للشركة الأم أو الفروع. فمثلا إذا تعرضت الشركة لسرقة بيانات العملاء ونتج عن ذلك رفع دعاوى قضائية من العملاء ضد الشركة فإنه يجب الإفصاح عن تفاصيل الدعوى القضائية بما فى ذلك إسم المحكمة التى ينظر فيها الدعوى وتواريخ الجلسات والأطراف الأساسية فى القضية وتوصيف لأساس إقامة الدعوى والطلبات.

سادسا: الإفصاح فى القوائم المالية

قد تؤثر حوادث الأمن السيبراني والمخاطر الناتجة عنها على القوائم المالية للشركة حيث يمكن أن تؤدي إلى:

- زيادة المصروفات المتعلقة بالتحقيق والإخطار بالإختراق وكيفية علاج ذلك وإمكانية التقاضي روما يرتبط بها من تكاليف الخدمات القانونية وغيرها من الخدمات المهنية الأخرى.
- إنخفاض الإيرادات حيث يتعين إما تقديم مزيد من الحوافز للعملاء للحفاظ عليهم وإلا يتم خسارتهم.
- المطالبات المتعلقة بالضمانات وعدم الوفاء بالعقد واسترجاع / استبدال المنتج والتعويضات الأطراف وزيادة أقساط التأمين.
- إنخفاض التدفقات النقدية المستقبلية أو إضمحلال الأصول الفكرية أو غير الملموسة وغيرها من الأصول بالإضافة إلى الإعتراف بمزيد من الالتزامات وزيادة تكاليف التمويل.

وبالتالى فإنه لا بد أن تقوم الشركات بتصميم نظم التقرير المالى ونظم الرقابة لها لتوفير ضمان معقول بأن المعلومات الخاصة بنطاق وحجم التأثيرات المالية لحوادث الأمن السيبراني ثم أخذها فى الإعتبار عند إعداد القوائم المالية في الوقت المناسب عندما تصبح المعلومات متاحة.

٥- دور مجلس الإدراة

يجب أن تقوم الشركة بالإفصاح عن طبيعة دور مجلس الإدارة فى إدارة مخاطر الأمن السيبرانى وبرنامج إدارة هذه المخاطر بالإشتراك مع إدارة الشركة والذى يكون له الأثر الإيجابى على المستثمرين فى قيام مجلس الإدارة بدوره كما يجب فى هذه المسائل الهامة.

وعن **العنصر الثانى** الخاص بالسياسات والإجراءات فقد شمل البنود التالية:

أولا: الإفصاح الخاص بالإجراءات والرقابات

تعتبر سياسات وإجراءات إدراة مخاطر الأمن السيبرانى عناصر أساسية فى إدراة مخاطر الشركات ولذلك يجب على الشركات التأكد من تطبيق سياسات وإجراءات شاملة تتعلق بالأمن السيبرانى والتأكد من كفاية الإجراءات والرقابات المتعلقة بالإفصاح عن الأمن السيبرانى وتقييم ما إذا كانت لديها ضوابط وإجراءات إفصاح كافية معمول بها لضمان أن المعلومات المتعلقة بحوادث ومخاطر الأمن السيبرانى يتم تسجيلها والإبلاغ عنها إلى الموظفين المناسبين وصولا إلى رئيس مجلس الإدارة لمساعدة الإدارة العليا فى إتخاذ القرارات التى تتعلق بتسهيل مهمة تصميم السياسات والإجراءات التى تمنع المديرين والمسئولين وغيرهم من التعاملات على أسهم الشركة نتيجة حصولهم على معلومات جوهرية عن مخاطر وحوادث الأمن السيبرانى غير المعلنة.

يجب على الشركات عند تصميم وتقييم الضوابط والإجراءات المتعلقة بالإفصاح النظر فيما إذا كانت هذه الضوابط والإجراءات سوف تمكن من الإفصاح بشكل مناسب عن المعلومات المتعلقة بمخاطر وحوادث الأمن السيبراني. فيجب أن تساعد هذه الإجراءات والضوابط الشركات فى تحديد المخاطر والحوادث السيبرانية وتقييم وتحليل تأثيرها على عمليات الشركة والسماح بقنوات الإتصال المفتوحة بين الخبراء الفنيين

وخبراء الإفصاح. ويجب على المدير التنفيذى والمدير المالى التأكد من تصميم وفعالية ضوابط وإجراءات الإفصاح والإفصاح عن ملخص لمدى كفاية وفعالية الضوابط والإجراءات والتأكد من عدم وجود أوجه قصور في ضوابط وإجراءات الإفصاح التي تجعلها غير فعالة.

٢- التداول من الداخل

يجب على الشركات ومديريها وموظفيها وغيرهم من الأطراف الداخلية ذات العلاقة مراعاة الامتثال للقوانين المتعلقة بالتداول من الداخل فيما يتعلق بالمعلومات غير المعلنة حول مخاطر وحوادث الأمن السيبراني بما في ذلك نقاط الضعف والإختراقات حيث يعتبر تداول هذه الأطراف على أساس معلومات جوهرية غير معلنة مخالفة للثقة والأمانة تجاه الشركة ومساهميها ولقوانين وقواعد التداول المعمول بها أثناء حيازتهم لتلك المعلومات غير المعلنة. ومن الضرورى أن يكون لدي الشركات سياسات وإجراءات مصممة جيدا لمنع تداول جميع أنواع المعلومات الجوهرية غير المعلنة بما في ذلك المعلومات المتعلقة بمخاطر وحوادث الأمن السيبراني. وتتطلب العديد من البورصات من الشركات المدرجة اعتماد قواعد السلوك والسياسات التي تعزز الامتثال للقوانين والقواعد واللوائح المعمول بها، بما في ذلك تلك التي تحظر التداول من الداخل على أساس المواد المعلومات غير المعلنة المتعلقة بمخاطر وحوادث الأمن السيبراني. كما يحظر التداول الداخلى أثناء فترة التحقيقات فى حوادث الأمن السيبرانى الجوهرية وقبل الإفصاح عن ذلك بإتخاذها التدابير الوقائية.

٣- التنظيمات والإفصاح الإنتقائى

يجب على الشركات أن يكون لديها إجراءات للتأكد من عدم الإفصاح بشكل انتقائي عن معلومات غير معلنة تتعلق بمخاطر وحوادث الأمن السيبراني قبل الإفصاح عن نفس المعلومات للجمهور (في حالة الإفصاح المقصود) أو على وجه السرعة (في حالة الإفصاح غير المقصود).

٣-أهم الجهود المصرية في دعم الأمن السيبراني

نصت المادة (٣١) من الدستور المصري (يناير ٢٠١٤) على أن: "أمن الفضاء المعلوماتي جزء أساسى من منظومة الأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه **على النحو الذي ينظمه القانون**". وبناءً على ذلك تم وضع الإستراتيجية الوطنية للأمن السيبرانى (٢٠١٧-٢٠٢١) ويتمثل **الهدف الإستراتيجى** لها فى مواجهة المخاطر السيبرانية وتعزيز الثقة فى البني التحتية للاتصالات والمعلومات وتطبيقاتها وخدماتها فى شتي القطاعات الحيوية وتأمينها من أجل تحقيق بيئة رقمية آمنة وموثوقة للمجتمع المصري بمختلف أطيافه". وتشتمل الاستراتيجية على **العناصر** الآتية:

١- **التحديات والأخطار السيبرانية** والتى تتمثل فى: خطر إختراق وتخريب البنى التحتية للاتصالات وتكنولوجيا المعلومات وخطر الإرهاب والحرب السيبرانية وخطر سرقة الهوية الرقمية والبيانات الخاصة.

٢- **أهم القطاعات الحيوية المستهدفة** وتشمل بالترتيب: قطاع الاتصالات وتكنولوجيا المعلومات، قطاع الطاقة وقطاع الخدمات الحكومية وقطاع النقل والمواصلات وقطاع الصحة وخدمات الإسعاف العاجل وقطاع الإعلام والثقافة، بالإضافة الي المواقع الرسمية للدولة والقطاعات ذات التأثير علي النشاط الاقتصادي مثل والتجارة والصناعة والزراعة والري والتعليم بمختلف مستوياته والاستثمار والسياحة.

٣- **العناصر الرئيسية لخطورة التهديدات السيبرانية:** استنادها الي تقنيات متقدمة ومتطورة، سرعة وسهولة انتشارها، اتساع نطاق تأثيرها.

٤- **ركائز الاستعداد/التوجه الاستراتيجى لمواجهة الأخطار السيبرانية:** الدعم السياسي والمؤسسي الاستراتيجي والتنفيذي، الاطار التشريعى، الإطار التنظيمي والتنفيذي، البحث العلمي والتطوير وتنمية صناعة الأمن السيبرانى، تنمية الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبرانى فى مختلف القطاعات، التعاون مع الدول الصديقة والمنظمات الدولية والاقليمية ذات الصلة، التوعية المجتمعية.

٥- تمثلت آلية التنفيذ فى تشكيل **المجلس الأعلى للأمن السيبراني** لحماية البني التحتية للاتصالات وتكنولوجيا المعلومات تحت اشراف وزارة الاتصالات وتكنولوجيا المعلومات وبرئاسة وزير الاتصالات والمجلس يتبع مجلس الوزراء من خلال وضع استراتيجية وطنية للأمن السيبرانى والاشراف على تنفيذها، مع ضرورة تحديثها فى ضوء التطورات التقنية المتلاحقة. تمثل فى المجلس الأطراف المعنية بالأمن القومي وبإدارة وتشغيل البني التحتية فى القطاعات الحيوية والمرافق العامة، وذوي الخبرة فى القطاع الخاص والجهات التعليمية والبحثية. وقد بدأ المجلس عمله التمهيدي فى يناير ٢٠١٥ وقام رئيس مجلس الوزراء باعتماد تشكيل المكتب التنفيذي للمجلس ولجنته الفنية وتوصيف مهامه فى يونيو ٢٠١٦.

٦- تتمثل أهم **البرامج الاستراتيجية فى المرحلة الحالية** (٢٠١٧-٢٠٢١) فى: برنامج لتطوير الاطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية وحماية الهوية الرقمية وبرنامج تطوير منظومة وطنية متكاملة لحماية أمن الفضاء السيبرانى وتأمين البني التحتية للاتصالات وتكنولوجيا المعلومات، برنامج لحماية الهوية الرقمية (برنامج المواطنة الرقمية) وتفعيل البني التحتية اللازمة لدعم الثقة فى التعاملات الالكترونية بوجه عام وفى الخدمات الحكومية الالكترونية بوجه خاص، برنامج لإعداد الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبرانى فى مختلف القطاعات، برنامج لدعم البحث العلمي والتطوير وتنمية صناعة الأمن السيبرانى، برنامج للتوعية المجتمعية بالفرص والمزايا التي

تقدمها الخدمات الالكترونية للأفراد والمؤسسات والجهات الحكومية وبأهمية الأمن السيبرانى لحماية تلك الخدمات من المخاطر والتحديات التي قد تواجهها.

هذا بالإضافة إلى اصدار قانون مكافحة جرائم تقنية المعلومات المعروف إعلامياً بـ"مكافحة جرائم الإنترنت ".

٤- دور المحاسبة فى إدارة مخاطر الأمن السيبرانى

تمثل المخاطر السيبرانية أحد مصادر الخطر الهامة بالنسبة للشركات. ومن أن أهم مخاطر التشغيل التى في عام ٢٠١٧ المخاطر السيبرانية وأمن البيانات (Kamiya et al., 2018, p.3) . وعلى الرغم من عدم وجود توافق في الآراء حول تعريف دقيق للمخاطر السيبرانية فإنها توصف بأنها "قدرات على تعطيل أو تدمير أو تهديد تقديم الخدمات الأساسية، أو استغلال نقاط الضعف لسرقة المعلومات والأموال من قبل الجهات الفاعلة السيبرانية والدول[٣]. ويعرفها معهد إدارة المخاطر بأنها "أي خطر يتعلق بحدوث خسائر مالية أو تعطيل أو ضرر لسمعة الشركة نتيجة تعطل أحد أنظمة تكنولوجيا المعلومات الخاصة بها[٤].

وتتلخص خطوات الإدارة الفعالة لمخاطر الأمن السيبرانى فى الخطوات التالية: (Eaton, 2019, p.3):

١- تحديد أولويات ومخاطر التعرض للأمن السيبرانى بالإستعانة بالخبرات فى تكنولوجيا المعلومات وتهديدات الأمن السيبراني الحالية.
٢- تصميم نظام رقابة وضوابط الأمن السيبراني ونظام رقابة تكنولوجيا المعلومات للتعامل مع المخاطر المحددة في المرحلة الأولى في ضوء أفضل ممارسات الصناعة الحالية ومعايير الرقابة (مثل معايير رقابة الأمن السيبراني للمعهد الأمريكى للمحاسبين القانونيين).

3 https://www.dhs.gov/cybersecurity-overview
4 https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/

٣- اختبار الفعالية التشغيلية لعناصر رقابة الأمن السيبرانيى من خلال اختبار ضوابط تكنولوجيا إما أثناء مراجعة القوائم المالية أو من خلال الخدمات الاستشارية فى مجال تكنولوجيا المعلومات أو المراجعة الداخلية.

٤- إعداد تقارير خارجية عن الأمن السيبراني وذلك وفقًا لمعايير خارجية مثل إطار تقرير المنشأة عن الأمن السيبراني للمعهد الأمريكى للمحاسبين القانونيين.

٥- الحصول على خدمات التأكيد من شركات المراجعة بخصوص فعالية برنامج إدارة مخاطر الأمن السيبراني للشركة والذى يتوقف على نجاح المراحل الأربع السابقة ويمكن إصدار تقارير خاصة بفعالية امج إدارة مخاطر الأمن السيبراني للشركة بدون إعلانه للأطراف الخارجية. أما إذا تم إعلانه خارجيا فلا يمكن لشركة المراجعة تقديم أية خدمات إستشارية فى المراحل الأربع السابقة لضمان إستقلال المراجع الخارجى.

الفرض الثالث:

فى ضوء الدراسات السابقة التى تم عرضها والجهود التى تمت على مستوى هيئة البورصة الأمريكية والمعهد الأمريكى للمحاسبين المعتمدين وعدم إصدار أية تنظيمات أو إرشادات مماثلة فى مصر فإنه يمكن إشتقاق فرض الدراسة الثالث كما يلى: "**يوجد إختلاف جوهرى بين طبيعة إفصاح شركات تكنولوجيا المعلومات المصرية والشركات الأمريكية فيما يتعلق بالأمن السيبرانى ومخاطره وإدارة هذه المخاطر**".

رابعا: الدراسة التطبيقية وإختبار الفروض:

١- الإفصاح عن الأمن السيبرانى وإدارة المخاطر.

تم إجراء دراسة مقارنة بين طبيعة الإفصاح عن الأمن السيبرانى ومخاطره فى التقارير والقوائم المالية للشركات المصرية المدرجة فى قطاع تكنولوجيا المعلومات حيث أنها الأكثر عرضة للهجمات والتهديدات السيبرانية وفقا للإستراتيجية الوطنية للأمن السيبرانى والأكثر خبرة بالأمن والهجمات والتهديدات السيبرانية، كما أنها مسئولة عن الأمن السيبرانى للشركات التى تقدم لها هذه الخدمات وبالتالى فهى أكثر الشركات التى من المفترض أن يكون لها السبق فى الإفصاح عن مثل هذه الأنشطة. ويمكن عرض النتائج كما يلى:

الشركة	الرمز	**الإفصاح عن برنامج إدارة المخاطر السيبرانية والحوادث السيبرانى (العنوان الإلكترونى على موقع مباشر مصر والموقع الإلكترونى للشركة)**
المؤشر للبرمجة ونشر المعلومات	AMPI	لا يوجد فى ٣١ مارس ٢٠١٩ https://www.mubasher.info/markets/EGX/stocks/AMPI http://www.al-moasher.net/Default.aspx
الشركة المصرية للأقمار الصناعية (نايل سات)	EGSA	فى ٣١ مارس لا يوجد https://www.mubasher.info/markets/EGX/stocks/EGSA http://www.nilesat.com.eg/
راية القابضة للإستثمارات المالية	RAYA	تم فحص التقرير السنوى فى ٣١ ديسمبر ٢٠١٨ كل ما ذكر عن الأمن السيبرانى فى أن الشركة تقود السوق فى تقديم أحدث التقنيات مثل حلول الشمول المالى والبيانات الضخمة وسلاسل الكتلة والأمن السيبرانى. ولم تذكر أية أنشطة تتعلق بإدارة المخاطر السيبرانية أو أية حوادث تعرضت لها الشركة. وكذلك تم فحص القوائم المالية عن الفترة المنتهية فى ٣١ مارس ٢٠١٩ ولم يحتوى على أية إفصاحات. https://www.mubasher.info/markets/EGX/stocks/RAYA http://rayacorp.com/

قناة السويس لتوطين التكنولوجيا	SCTS	لا يوجد أية إفصاحات فى القوائم المالية فى ٣١ مارس ٢٠١٩ https://www.mubasher.info/markets/EGX/stocks/SCTS http://www.scts-eg.com/AR
فوري لتكنولوجيا البنوك والمدفوعات الالكترونية	FWRY	لا يوجد أية إفصاحات فى القوائم المالية فى ٣١ مارس ٢٠١٩ https://www.mubasher.info/markets/EGX/stocks/FWRY/profile https://fawry.com/news-disclosures/
فرتيكا للصناعة والتجارة	VERT	لا يوجد أية إفصاحات فى القوائم المالية فى ٣١ مارس ٢٠١٩ http://www.verti-ka.com/ https://www.mubasher.info/markets/EGX/stocks/VERT/financial-statements
راية لخدمات مراكز الاتصالات	RACC	لا يوجد أية إفصاحات فى القوائم المالية فى ٣١ مارس ٢٠١٩ http://rayaholding.com/investor-relations/
فاروتك لانظمة التحكم والاتصالات	PTCC	لا يوجد أية إفصاحات فى القوائم المالية فى ٣١ مارس ٢٠١٩ https://www.mubasher.info/markets/EGX/stocks/PTCC http://ww6.pharaoh-tech.com/

التحليل

يتضح من الجدول السابق **ضعف** الإفصاح عن أنشطة الأمن السيبرانى ومخاطره وبرامج إدارة هذه المخاطر، لذلك تم إختيار البنك التجارى الدولى بإعتباره أفضل بنك تجارى يقوم بالإفصاح عن مثل هذه الأنشطة نظرا لحصوله على العديد من الجوائز فى مجال التحول الرقمى وإستخدام الإنترنت وأمن المعلومات وبالتالى فإنه من المتوقع أن يتم الإفصاح عن بعض أنشطة الأمن السيبرانى لمواجهة مخاطر التحول الرقمى حيث حصل البنك فى عام ٢٠١٨ على جائزة بنك التميز الرقمى فى مصر وجائزة أفضل إدارة نقدية عبر الإنترنت فى مصر وجائزة أفضل خدمات البوابة الإلكترونية في مصر وجائزة أفضل أمن المعلومات وإدارة

الاحتيال في مصر إلا أنه بفصح القوائم المالية للبنك فى العام المنتهى فى ٣١ ديسمبر ٢٠١٨ وتقرير الحوكمة والموقع الإلكترونى للبنك تبين عدم الإشارة إلى أية معلومات تتعلق بالأمن السيبرانى وكل ما ذكر أنه يوجد "**لجنة العمليات وتكنولوجيا المعلومات**" وهى لجنة مستقلة تابعة لمجلس الإدارة لمعاونة المجلس في القيام بدوره على الوجه الأمثل. وبناءً عليه يلتزم مجلس الإدارة بتوفير كافة الموارد والمعلومات اللازمة والتي من شأنها مساعدة هذه اللجنة في أداء واجبها على نحوٍ فعال. ويخضع عمل اللجنة إلى ميثاق مهني مكتوب يتضمن مسئوليات ومتطلبات وقواعد تشكيل اللجنة، وتقوم اللجنة بصياغة الاستراتيجية الخاصة بالقطاعين مع تحديد المخاطر المتعلقة بهما. كما تقوم اللجنة باعتماد الاستثمارات الخاصة بتلك المشروعات المتعلقة بتكنولوجيا المعلومات.

ومما تقدم يتبين ضعف الإفصاح عن أنشطة الأمن السيبرانى أو أية تهديدات أو هجمات تعرضت لها الشركات أو تم التقرير عنها بالنسبة للشركات المصرية المسجلة فى قطاع تكنولوجيا المعلومات، وكذلك قطاع البنوك، وبالمقارنة مع الشركات الأمريكية حول طبيعة الإفصاح عن أنشطة الأمن السيبرانى وما يرتبط بها من تهديدات ومخاطر وخاصة فى شركة Microsoft وشركة Netflix وشركة Facebook كما يتضح من العرض التالى.

-**شركة مايكروسوفت:** هى شركة متعددة الجنسيات تعمل في مجال تقنيات الحاسوب، يبلغ عائدها لسنة ٢٠١٦ أكثر من ٨٥ مليار دولار، ويعمل بها ١١٤,٠٠٠ موظف (٢٠١٦) وهي أكبر مصنع للبرمجيات في العالم من ناحية العائدات اعتباراً من عام ٢٠١٦. تطوّر وتصنِّع وترخِّص مدى واسعا من البرمجيات للأجهزة الحاسوبيّة. يقع المقر الرئيسي للشركة في ولاية واشنطن، الولايات المتحدة. كان بيل جيتس وبول ألين هما المؤسسين والملاك لهذه الشركة قبل أن تصبح من الشركات العامة والمتداولة في أسواق الأسهم (NASDAQ Website).

وبفحص التقرير السنوى للشركة (10-k) الذى قدمته الشركة إلى هيئة البورصة الأمريكية والموجود على الموقع الإلكترونى للشركة وعلى موقع NASDAQ ورد به ما يلى: أن الشركة ترى أن النطاق السحابي العالمي بالإضافة إلى المجموعة الواسعة من حلول لمشكلات الأمن التى تقدمها الشركة تتيح لها فرصة حل تحديات الأمن السيبراني المعقدة بفعالية لعملاء الشركة ويعطيها ميزة تنافسية.

كما ورد فى النموذج أن الهجمات الإلكترونية ونقاط الضعف الأمنية يمكن أن تؤدي إلى انخفاض الإيرادات أو زيادة التكاليف أو مطالبات المسئولية أو إلحاق الضرر بسمعة الشركة أو مركزها التنافسي. وورد أيضا أنه يوجد تطور للتهديدات السيبرانية باستمرار، مما يزيد من صعوبة اكتشافها والدفاع عنها بنجاح وأنه قد لا تكون لدي الشركة قدرة حالية على اكتشاف بعض الثغرات الأمنية مما قد يسمح لها بالاستمرار في بيئة عمل الشركة على مدى فترات زمنية طويلة. ويمكن أن يكون لتهديدات الإنترنت آثار متتالية تتزايد مع زيادة السرعة عبر الشبكات الداخلية للشركة وأنظمتها وتلك الخاصة بشركاء الشركة وعملائها. ويمكن أن تؤدي انتهاكات منشآت الشركة أو شبكتها أو أمان البيانات لها إلى تعطيل أمان الأنظمة وتطبيقات الأعمال للشركة، مما يضعف قدرة الشركة على تقديم الخدمات لعملائها وحماية خصوصية بياناتهم، ويؤدي إلى تأخير في تطوير المنتجات أو الإضرار بمعلومات الأعمال السرية أو الفنية مما يلحق الأذى بسمعة الشركة ومركزها التنافسي ، أو نتيجة لسرقة أو سوء استخدام الممتلكات الفكرية أو غيرها من الأصول للشركة، وهذا يتطلب تخصيص المزيد من الموارد للتقنيات المحسنة وإلا سيكون التأثير سلبًا على أعمال الشركة.

وتم الإشارة إلى أنه بالنسبة لأمان منتجات وخدمات وأجهزة وبيانات العملاء للشركة فإنه نظرا لأن الشركة تدمج بشكل متزايد البرمجيات مفتوحة المصدر في منتجاتها فإنه قد تكون هناك ثغرات في البرامج مفتوحة المصدر تجعلها عرضة للهجمات الإلكترونية.

وورد أنه قد ترى سلطات حماية البيانات أن جمع بيانات العملاء الخاصة بنا واستخدامها وإدارتها لا يتوافق مع قوانينها ولوائحها مما قد يؤدي إلى إجراء تشريعي أو تنظيمي متعلق بمتطلبات الأمن السيبراني يؤدى إلى زيادة تكاليف تطوير أو توفير أو تأمين منتجاتنا وخدماتنا.

كما يمكن أن تؤدى الأحداث الكارثية أو الظروف الجيوسياسية geopolitical إلى تعطل أعمال الشركة فقد يتسبب تعطل أو فشل أنظمة أو عمليات الشركة بسبب حدوث زلزال كبير أو حدث طقس أو **هجوم إلكتروني** أو حدث كارثي آخر يتسبب في تأخير إتمام المبيعات أو تقديم الخدمات أو أداء وظائف مهمة أخرى.

ويتضح من العرض السابق **إختلاف** طبيعة الإفصاح عن أنشطة الأمن السيبرانى ومخاطر وتهديدات الهجمات والحوادث الإلكترونية فى شركات تكنولوجيا المعلومات المصرية والأمريكية وذلك متوقع نتيجة إصدار هيئة سوق المال الأمريكية دليل إسترشادى للشركات بالإفصاح عن هذه الأنشطة بينما لم يصدر أية إرشادات من الهيئة العامة للرقابة المالية أو البورصة المصرية أو البنك المركزى المصرى للبنوك التابعه له على الرغم من أنها الأكثر تعرضا لهذه المخاطر. ولكن لم يتم الإشارة فى نموذج (k–10) إلى كيف يمكن للشركة مواجهة المخاطر المتزايدة من التهديدات والحوادث السيبرانية. وبالتالى **قبول** فرض الدراسة **الثالث** بأنه: "**يوجد إختلاف جوهرى بين طبيعة إفصاح شركات تكنولوجيا المعلومات المصرية والشركات الأمريكية فيما يتعلق بالأمن السيبرانى ومخاطره وإدارة هذه المخاطر**

تم إجراء مزيد من التحليل على الشركات العالمية التى تعرضت لأكبر وأخطر الهجمات السيبرانية ومنها: شركة فيسبوك فى سبتمبر ٢٠١٨ وشركة Netflix فى ٢١ أكتوبر ٢٠١٦.

-**شركة فيسبوك:** أفصحت الشركة فى التقرير المالى لها الربع سنوى عن الفترة المنتهية فى ٣٠ سبتمبر ٢٠١٨ أنها تعرضت لهجوم سيبرانى تابع لجهة خارجية من خلال استغلال ثغرة أمنية في شفرة Facebook لسرقة رموز وصول المستخدم والتي تم استخدامها بعد ذلك للوصول إلى بعض معلومات الملف الشخصي

لحوالي ٢٩ مليون حساب مستخدم على Facebook فى سبتمبر ٢٠١٩. وقد اتخذت الشركة خطوات لتصحيح الهجوم بما في ذلك إصلاح المشكلة وإعادة تعيين رموز وصول المستخدم وإخطار المستخدمين المتأثرين. وقد يؤدى هذا الحدث إلى ضياع الثقة في العلامة التجارية للشركة. بالإضافة إلى أن الأحداث المحيطة بهذا الهجوم السيبراني أصبحت موضوعًا للجنة حماية البيانات الأيرلندية ولجنة التجارة الفيدرالية الأمريكية وغيرها من استفسارات الحكومات في الولايات المتحدة وأوروبا والولايات القضائية الأخرى. ولذلك فإن الشركة عرضة إلى غرامات وتكاليف كبيرة أو تتطلب منا تغيير ممارسات أعمالنا، أو التأثير سلبًا على أعمالنا. ولذلك تم رفع دعاوى جماعية متعددة في المحاكم ضد الشركة اعتبارا من ٢٨ سبتمبر ٢٠١٨ بدعوى حدوث انتهاكات لقوانين حماية المستهلك وغيرها من أسباب الدعوى فيما يتعلق بالهجوم السيبراني من جهة خارجية والمطالبة بالحصول على تعويضات غير محددة.

ومن خلال فحص التقارير المالية للشركة تبين أن لذلك الهجوم العديد من الآثار السلبية على سعر السهم للشركة وحجم التداول وصافى الدخل وبالتالى العائد على السهم. ويمكن عرض ذلك كما يلى[٥]:

١- الأثر على سعر السهم:

يتضح من الجدول التالى أن سعر سهم شركة فيسبوك قد انخفض بنسبة وصلت إلى ٢٣% تقريبا من سعر السهم خلال شهر من حدوث الإختراق السيبرانى حيث انخفضت من ١٦١,٠٣ دولار فى ٢٠١٨/٩/٢٤ إلى ١٢٣,١ دولار فى ٢٠١٨/١٢/٢٤

التاريخ	السعر	التغير التراكمى فى السعر
٢٠١٨/٩/٢٤	١٦١,٠٣	(%٣,٣٧)
٢٠١٨/١٠/١١	١٥٠,١٣	(%٥,٦٤)
٢٠١٨/١٠/٢٥	١٤٧,٧٣	(%٦,٩٣)

[٥] تم الحصول على البيانات من الموقع الرسمى للشركة ومن موقع https://finance.yahoo.com/quote/FB/analysis?p=FB ومن موقع البورصة الأمريكية Nasdaq

٢٠١٨/١١/٢٠	١٢٧,٠٣	(%٢٠,٨٣)
٢٠١٨/١٢/٢٤	١٢٣,١	(%٢٢,٧٨)

٢- الأثر على حجم التداول:

يتضح من الجدول التالى أن حجم التداول لشركة فيسبوك قد انخفض بنسبة وصلت إلى ٥٨% تقريبا خلال شهر من حدوث الإختراق السيبرانى حيث انخفضت من ٢٢٤٦٥٢٠٠ سهم فى ٢٠١٨/٩/١٨ و١٩٦٢٩٠٠٠ سهم فى ٢٠١٨/٩/١٩ إلى ١١٨٨٦١٠٠ فى ٢٠١٨/١٢/٢٤

التاريخ	حجم التداول	التغير التراكمى فى حجم التداول
٢٠١٨/٩/١٩	١٩٦٢٩٠٠٠	(%١٢,٦٢)
٢٠١٨/٩/٢٤	١٩٢٢٢٨٠٠	(%١٤,٦٩)
٢٠١٨/١٠/٩	١٨٨٤٤٤٠٠	(%١٦,٦٦)
٢٠١٨/١٠/١٥	١٥٤٣٣٥٠٠	(%٣٤,٧٦)
٢٠١٨/١١/٢٣	١١٨٨٦١٠٠	(%٥٧,٧٥)

وبالنسبة للأثر على **صافى الدخل** فقد انخفض فى أول فترة بعد حادث الإختراق السيبرانى بنسبة ٦٤,٧١% من ٦٨٨٢٠٠٠ مليون دولار فى ٢٠١٨/١٢/٣٠ إلى ٢٤٢٩٠٠٠ مليون دولار فى ٢٠١٩/٣/٣٠، **وانخفض العائد على السهم** من ١,٧٨ دولار للسهم إلى ٠,٨٥ دولار للسهم أى انخفض بنسبة ٥٢,٢٥%. ويعرض الجدول التالى الفرق بين توقعات المحللين للعائد على السهم والعوائد الفعلية للربع

الأول والربع الثانى من ٢٠١٩ والذى يوضح أن نسبة الإختلاف وصلت إلى ٤٩% إنخفاض أقل من المتوقع فى ٢٠١٨/٣/٣٠ و٥٢% فى ٢٠١٩/٣/٣٠:

التاريخ	٢٠١٨/٣/٣٠	٢٠١٩/٣/٣٠
العائد على السهم المتوقع	١,٦٣	١,٨٨
العائد على السهم الفعلى	٠,٨٥	٠,٩١
الفرق	٠,٧٨-	٠,٩٧-
نسبة الإختلاف	%٤٧,٩-	%٥١,٦-

٢-شركة Netflix: هي شركة ترفيهية أمريكية تم تأسيسها في ٢٩ أغسطس ١٩٩٧، في كاليفورنيا. تتخصص في تزويد خدمة البثّ الحي والفيديو حسب الطلب وتوصيل الأقراص المدمجة عبر البريد. في عام ٢٠١٣ توسعت شركة نتفليكس بإنتاج الأفلام والبرامج التلفزيونية، وتوزيع الفيديو عبر الإنترنت. وقد أعلنت عن حدوث **هجوم سيبرانى بتاريخ ٢٠١٦/١٠/٢١**. وفيما يلى تحليلا لأثر الإفصاح عن الهجوم السيبرانى فى ٢١ أكتوبر ٢٠١٦ على سعر السهم وحجم التداول للشركة.

أولا: أثر الإفصاح عن مخاطر الأمن السيبرانى على سعر السهم:

يوضح الجدول التالى أثر إفصاح الشركة فى ٢١ أكتوبر عن تعرضها لهجمة سيبرانية:

التاريخ	سعر السهم	التغير التراكمى فى سعر السهم
٢٠١٦/١٠/٢٤	١٢٧,٣٣	(%٠,١٣)
٢٠١٦/٩/٢٤	١٢٦,٥١	(%٠,٦٤)
٢٠١٦/١١/١	١٢٣,٣	(%٢ ,٥٤)

٢٠١٦/١١/١٠	١١٥,٤٢	(%٦,٣٩)
٢٠١٦/١١/١٥	١١٣,٥٩	(%١,٥٩)
الأثر الإجمالى على سعر السهم		(%١١,٢٩)

يتضح من الجدول السابق أن سعر سهم شركة Netflix قد انخفض بنسبة وصلت إلى ١٢% تقريبا خلال شهر من حدوث الإختراق السيبرانى حيث انخفضت من ١٢٧,٣٣ دولار فى ٢٠١٦/١٠/٢٤ إلى ١١٣,٥٩ دولار فى ٢٠١٨/١٢/٢٤.

ثانيا: أثر الإفصاح عن مخاطر الأمن السيبرانى على حجم التداول:

التاريخ	حجم التداول	التغير فى حجم التداول
[٦]٢٠١٦/١٠/٢٤	١٥٩٨٠٧٠٠	(%١٥,١٤)
٢٠١٦/١٠/٢٥	٨٢٥٣٩٠٠	(%٤٨,٣٥)
٢٠١٦/١٠/٢٧	٦٩١٤٢٠٠	(%١٦,٢٣)
٢٠١٦/١٠/٣١	٦٥١٧٥٠٠	(%٥,٧٤)
٢٠١٦/١١/٢٣	٤٨١٦٥٠٠	(%٢٦,١)
٢٠١٦/١١/٨	٤٦٩٠٨٠٠	(%٢,٦١)
٢٠١٦/١١/٢٣	٤٥٢١٣٠٠	(%٣,٦١)
٢٠١٦/١١/٢٥	١٦١٦٣٠٠	(%٦٤,٢٥)

[٦] أول يوم عمل بعد الهجوم السيبرانى الذى حدث فى ٢١ أكتوبر ٢٠١٦.

التغير التراكمى من ٢٠١٦/١٠/٢٤ إلى ٢٠١٦/١١/٢٥		**(٩١,٤٢%)**

يتضح من الجدول السابق أن حجم التداول لشركة Netflix قد انخفض بنسبة وصلت إلى ٩١% تقريبا خلال شهر من حدوث الإختراق السيبرانى حيث انخفضت من ١٥٩٨٠٧٠٠سهم فى ٢٠١٦/١٠/٢٤ إلى ١٦١٦٣٠٠ فى ٢٠١٦/١١/٢٥.

وفى ضوء النتائج السابقة لأثر الإفصاح عن مخاطر الأمن السيبرانى على أسعار الأسهم وأحجام التداول لشركتى Facebook و Netflix يتبين وجود آثار سلبية جوهرية للإفصاح على أسعار الأسهم وأحجام التداول للشركتين محل الدراسة وبالتالى رفض **الفرض الأول** بأنه: "لا يوجد تأثير جوهرى للإفصاح عن مخاطر الأمن السيبرانى على أسعار الأسهم " وقبول الفرض البديل " يوجد تأثير جوهرى للإفصاح عن مخاطر الأمن السيبرانى على أسعار الأسهم" وأن هذا التأثير سلبياً، حيث إنخفضت أسعار الأسهم بشكل كبير بنسبة بلغت **١١,٢٩% لشركة Netflix** خلال شهر واحد فقط و ٦,٩٣% لشركة فيسبوك خلال شهر واحد فقط و ٢٢,٧٨% خلال شهرين. ويجب ملاحظة أنه تم حساب الأثر التراكمى خلال ٣٠ يوم و٦٠ يوم للتأكيد على أن الإتجاه لم يتغير بعد يومين أو ثلاثة أيام أو أسبوع كما أشارت بعض الدراسات السابقة إلى أنه يمكن أن يحدث تغيير فى أسعار التداول ولكنها سرعان ما تتلاشى بمرور الوقت وتستعيد الأسهم أسعارها الطبيعية.

وكذلك رفض **الفرض الثانى:** " يؤدى الإفصاح عن مخاطر الأمن السيبرانى إلى زيادة حجم التداول بشكل جوهري" وقبول الفرض البديل " يؤدى الإفصاح عن مخاطر الأمن السيبرانى إلى إنخفاض أحجام التداول بشكل جوهري" حيث إنخفضت أحجام التداول بشكل كبير بنسبة بلغت **٩١,٤٢%** لشركة Netflix خلال شهر واحد فقط و٣٤,٧٦% لشركة Facebook خلال شهر واحد فقط و٥٧,٧٥% خلال شهرين. ويجب

ملاحظة أنه تم حساب الأثر التراكمى خلال ٣٠ يوم و٦٠ يوم للتأكيد على أن الإتجاه لم يتغير بعد يومين أو ثلاثة أيام أو أسبوع كما أشارت بعض الدراسات السابقة إلى أنه يمكن أن يحدث تغيير فى أحجام التداول ولكنها سرعان ما تتلاشى بمرور الوقت وتستعيد الأسهم أحجام التداول الطبيعية.

النتائج والتوصيات والدراسات المستقبلية

أولا: النتائج:

١- **رفض فرض الدراسة الأول** بأنه لا يوجد تأثير جوهرى للإفصاح عن مخاطر الأمن السيبرانى على أسعار الأسهم حيث تبين وجود أثر جوهرى للإفصاح عن مخاطر الأمن السيبرانى على إنخفاض أسعار الأسهم لشركتى Facebook و Netflix.

٢- **رفض فرض الدراسة الثانى** بأنه يوجد تاثير جوهرى للإفصاح عن مخاطر الأمن السيبرانى على زيادة أحجام التداول للأسهم حيث تبين وجود أثر سلبى نتيجة إنخفاض أحجام التداول لشركتى Facebook و Netflix بشكل جوهرى.

٣- **قبول فرض الدراسة الثالث** بأنه يوجود فرق جوهرى فى طبيعة الإفصاح بين الشركات المصرية المسجلة فى قطاع تكنولوجيا المعلومات والشركات الأمريكية المسجلة فى قطاع الإتصالات وتكنولوجيا المعلومات وهذا متوقع نتيجة وجود إرشادات لدعم الشركات فى الإفصاح عن أنشطة ومخاطر الأمن السيبرانى وإطار للتقرير عن مخاطر الأمن السيبرانى الصادر عن AICPA.

٤- ضعف الإفصاح عن الأمن السيبرانى ومخاطره وكيفية إدارة هذه المخاطر فى شركات تكنولوجيا المعلومات وكذلك القطاع المالى فى مصر.

٥- يوجد العديد من الآثار الإيجابية للإفصاح عن مخاطر الأمن السيبرانى على سعر السهم وعلى القيمة السوقية للشركة وخفض جرائم وحوادث الأمن السيبرانى.

٦- عدم إصدار أية تنظيمات أو إرشادات للشركات المصرية المسجلة تدعم الشركات فى الإفصاح عن مخاطر الأمن السيبرانى وبرامج إدارة مخاطره حيث تعتبر الإستراتيجية الوطنية للأمن السيبرانى عامة وغير موجهة للشركات المسجلة فى سوق الأوراق المالية.

ثانيا: التوصيات:

١- إصدار الهيئة العامة للرقابة المالية دليلا استرشاديا للأمن السيبراني يتم من خلاله تحديد الضوابط المتعلقة بالأمن السيبراني التي تساعد على تحسين إدارة مخاطر الأمن السيبراني من خلال تبني أفضل الممارسات العالمية وتشريعات أمن سيبرانية محلية.

٢- يجب على إدارات الشركات إنشاء نظام قوى لحوكمة الأمن السيبرانى.

١- قيام إدارات الشركات بتأمين تعاملاتها الإلكترونية ضد الاختراقات والقرصنة الإلكترونية خصوصًا أن هناك توسعا واضحا فى الاعتماد على التكنولوجيا فى ظل الثورة الصناعية الرابعة.

٣- قيام إدارات الشركات بإنشاء لجنة متخصصة بالأمن السيبرانى.

٤- قيام إدراة المراجعة الداخلية بدورها فى تحسين الأمن السيبرانى من خلال توفير الرقابات الداخلية المناسبة لذلك.

٥- يجب على الهيئة العامة للرقابة المالية إلزام الشركات المسجلة بالإنفاق على أنشطة الأمن السيبرانى بمبالغ محددة.

٦- الإهتمام بتنمية مهارات والتطوير المهنى لأعضاء فريق المراجعة الداخلية حتى تتوافر لديهم الكفاءات المطلوبة لتحقيق الأمن السيبرانى ومواكبة التطور التكنولوجى فى بيئة الأعمال الحديثة من خلال حصولهم على شهادات مهنية فى الأمن السيبرانى.

٧- تضمين المقررات الدراسية المتخصصة لمرحلتى البكالوريوس والدراسات العليا خاصة بالأمن السيبرانى والإهتمام بوجود تخصصات مشتركة بينية interdisciplinary بين المحاسبة ونظم أمن المعلومات.

٨- مطالبة المجلس الأعلى للجامعات بإضافة مقررات دراسية كمتطلب جامعة فى الأمن السيبرانى لا تدخل فى المجموع النهائى ويمكن استثناء الكليات المتخصصة مثل الحاسبات والمعلومات.

٩- إلزام الشركات المسجلة فى البورصة المصرية بإصدار تقرير عن الأمن السيبرانى يتضمن: المخاطر السيبرانية التى تعرضت لها والآثار المختلفة لها ومراجعته بشكل مستقل.

١٠- يجب على شركات المحاسبة الكبرى القيام بدورها فى تقديم الإستشارات والخدمات التى تدعم الشركات فى تأمين أنشطتها السيبرانية المختلفة ونظم الرقابة الداخلية وتكنولوجيا المعلومات.

١١- يجب على مجلس معايير المراجعة الدولية IASB إصدار معيار ينظم جوانب المراجعة فيما يتعلق بالأمن السيبرانى وإصدار تقرير مستقل للمراجع عن الأمن السيبرانى لزيادة ثقة المستثمرين.

دراسات مستقبلية:

أثر الإفصاح الإختيارى عن إختراقات الأمن السيبرانى على قيمة الشركة ، العلاقة بين الإفصاح عن الأمن السيبرانى والتعاملات الداخلية على الأسهم، دور إدارة المراجعة الداخلية فى إدارة مخاطر الهجمات السيبرانية، دور المراجع الخارجى فى تقديم الإستشارات وخدمات التأكيد عن أنشطة ومخاطر الأمن السيبرانية. المخاطر السيبرانية والإستحواذ، أثر الحوادث السيبرانية على تقرير المراجع الخارجى وأتعاب عملية المراجعة، أثر الإفصاح عن المخاطر السيبرانية على قيمة الشركات عند الإندماج والإستحواذ.

المراجع

أولا: مراجع باللغة العربية:

١- الإستراتيجة الوطنية للأمن السيبرانى، (٢٠١٧) ، المجلس الأعلى للأمن السيبرانى، رئاسة مجلس الوزراء جمهورية مصر العربية.
٢- تعليمات التكيف مع المخاطر السيبرانية، (٢٠١٨)، البنك المركزى الأردنى.
٣- الدليل الإسترشادي للأمن السيبراني لمؤسسات السوق المالية، (٢٠١٩)، هيئة السوق المال السعودية.

ثانيا: مراجع باللغة الإنجليزية:

1- American Institute of Certified Public Accountants (AICPA). 2017a. SOC for Cybersecurity: A Backgrounder. New York, NY: AICPA.
2- American Institute of Certified Public Accountants (AICPA). 2017b. Illustrative Cybersecurity Risk Management Report. New York, NY: AICPA.
3- American Institute of Certified Public Accountants (AICPA). 2017c. AICPA Unveils Cybersecurity Risk Management Reporting Framework. Available at:https://www.aicpa.org/press/pressreleases/2017/aicpa-unveils-cybersecurityrisk-management-reporting-framework.html
4- Amir, E., Levi, S. and Livne, T. (2018), "Do firms underreport information on cyber-attacks? Evidence from capital markets", *Review of Accounting Studies*, Vol. 23 No. 3, pp. 1177-1206.
5- Cavusoglu H, Mishra B, Raghunathan S., (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerice*. Vol. 9(1). pp.69–104.
6- Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and Cybersecurity Risk Management. *Current Issues in Auditing*, 13(2), C1-C9.
7- Ettredge, M.L., Guo, F. and Li, Y. (2018), "Trade secrets and cyber security breaches", *Journal of Accounting and Public Policy*, Vol. 37 No. 6, pp. 564-585.
8- Gansler, J. and Lucyshyn, W. (2005), Improving the security of financial management systems: what are we to do? , *Journal of Accounting and Public Policy*, Vol. 24 No. 1, pp. 1-9.
9- Goel, S., and H. A. Shawky. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, vol.46, pp.404–410.
10- Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2003), "Sharing information on computer systems security: an economic analysis", *Journal of Accounting and Public Policy*, Vol. 22 No. 6, pp. 461-485.

11- Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Sohail, T. (2006), The impact of the Sarbanes-Oxley act on the corporate disclosures of information security activities, *Journal of Accounting and Public Policy*, Vol. 25 No. 5, pp. 503-530.

12- Gordon, L.A., Loeb, M.P. and Sohail, T. (2010), "Market value of voluntary disclosures concerning information security", *MIS Quarterly*, Vol. 34 No. 3, pp. 567-594.

13- Gwebu, K. L., J. Wang, and L. Wang. 2018. The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information systems*, 35(2): 683714.

14- Gyun No, W. and Vasarhelyi, M.A. (2017), Cybersecurity and continuous assurance, *Journal of Emerging Technologies in Accounting*, Vol. 14 No. 1, pp. 1-12.

15- Haapamäki, E., & Sihvonen, J. (2019), Cybersecurity in accounting research, *Managerial Auditing Journal*, 34(7), pp.808-834.

16- Heller, M. (2017). "Cyber attacks can cause major stock drops." CFO.com April 12, 2017.

17- Higgs, J. L., R. E. Pinsker, T. J. Smith, and G. R. Young. (2016). The relationship between board level technology committees and reported security breaches. Journal of Information Systems 30(3): 79-98

18- Hinz, O., M. Nofer, D. Schiereck, and J. Trillig. 2015. The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management* 52: 337-347

19- Kammoun, N., Bounfour, A., Özaygen, A., & Dieye, R. (2019). Financial market reaction to cyberattacks. *Cogent Economics & Finance*, Vo. 7(1), 1645584.

20- Kashmiri, S., C. D. Nicol, and L. Hsu. (2017). Birds of a feather: Intra-industry spillover of the Target customer data breach and the shielding role of IT, marketing, and CSR. *Journal of the Academy of Marketing Science* 45(2): 208-228.

21- Kelton, A. S., & Pennington, R. R. (2019). Do voluntary disclosures mitigate the cybersecurity breach contagion effect?, *Journal of Information Systems*, In-Press. Available at: https://doi.org/10.2308/isys-52628.
22- Lange R, Burger EW. (2017). Long-term market implications of data breaches. *Journal of Information Privacy and Security*.forthcoming.
23- Li, H., No, W. and Wang, T. (2018), "SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors", *International Journal of Accounting Information Systems*, Vol. 30, pp. 40-55.
24- Lin, Z., Sapp, T. R., Ulmer, J. R., & Parsa, R. (2019). Insider Trading Ahead of Cyber Breach Announcements. *Journal of Financial Markets*, 100527.
25- Richardson, V., Watson, M. W., & Smith, R. E. (2019). Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches. *Journal of Information Systems*, Vol. 33, No. 3, pp. 227-265.
26- Rosati, P., Cummins, M., Deeney, P., Gogolin, F., van der Werff, L. & Lynn, T., (2017).The effect of data breach announcements beyond the stock price: Empirical evidence on market activity, *International Review of Financial Analysis*, V.49, pp.146-154
27- Spanos, G., and L. Angelis. 2016. The impact of information security events to the stock market: *A systematic literature review. Computers & Security*, vol.58, pp.216–229.
28- Wang, Y., Kannan, K. and Ulmer, J. (2013), "The association between the disclosure and the realization of information security risk factors", *Information Systems Research*, Vol. 24 No. 2, pp. 201-218.

ثانيا: مواقع إلكترونية:

29- https://ar.wikipedia.org/wiki/%D9%82%D8%A7%D8%A6%D9%85%D8%A9_%D8%A7%D9%84%D8%B4%D8%B1%D9%83%D8%A7%D8%AA_%D8%A7%D9%84%D9%85%D8%B5%D8%B1%D9%8A%D8%A9#%D8%AA%D9%83%D9%86%D9%88%D9%84%D9%88%D8%AC%D9%8A%D8%A7_%D8%A7%D9%8

4%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA at 20 January, 2019.
30- https://www.cibeg.com/Arabic/InvestorRelations/CompanyStructure/Pages/BoardCommittees.aspx.accessed at 22 February, 2019.
https://www.constituteproject.org/constitution/Egypt_2014.pdf?lang=ar
31- https://www.microsoft.com/en-us/Investor/sec-filings.aspx. at 15 February, 2018.
32- https://www.mubasher.info/countries/eg/companies at 15 March, 2019.
33- http://rayaholding.com/investor-relations/ at 22 March, 2019.
34- https://cma.org.sa/MediaCenter/PR/Pages/Cybersecurity_.aspx at 16 January, 2019.
35- http://www.cbj.gov.jo/DetailsPage/CBJAR/NewsDetails.aspx?ID=213 at 22 March, 2019.
36- https://finance.yahoo.com/quote/FB/analysis?p=FB at 13 January, 2019.
37- https://finance.yahoo.com/quote/NFLX/financials?p=NFLX at 13 February, 2019.
38- http://www.netflix.com at 13 February, 2019.

ثالثا: مصادر أخرى:

1- Berr J. Equifax breach exposed data for 143 million consumers, (2017). *CBS News*.
2- Bianchi, D., & Tosun, O. K. (2019). Cyber attacks and stock market activity. *WBS Finance Group Research Paper No. 251*. Available at SSRN: https://ssrn.com/abstract=3190454 or http://dx.doi.org/10.2139/ssrn.3190454
3- CISCO, (2017). Annual Cybersecurity Report.

4- Cybersecurity Ventures. (2017). Cybercrime Report. https://cybersecurityventures.com/2015-wp/wp content/uploads/2017/10/2017-CybercrimeReport.pdf
5- Collins K. Yahoo and Equifax just proved that you can never trust the first number announced in the data, (2017). *Quartz*.
6- Gwebu, K. L., J. Wang, and W. Xie. (2014). Understanding the cost associated with data security breaches. Pacific Asia Conference on Information Systems 2014 Proceedings
7- Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2018). What is the impact of successful cyberattacks on target firms? (No. w24409). National Bureau of Economic Research.PwC. 2017. 20th CEO Survey. Available at: https://www.pwc.com/gx/en/ceo-survey/2017/pwcceo-20th-survey-report-2017.pdf.
8- Rubin, G. (2019). Many company hacks go undisclosed to SEC despite regulator efforts. *Wall Street Journal*, (February 26).
9- Securities and Exchange Commission (SEC). 2011. CF Disclosure Guidance: Topic No. 2, Cybersecurity (October 13, 2011). Available at https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
10- Securities and Exchange Commission (SEC). (2018). Commission Statement and Guidance on Public Company Cybersecurity Disclosures Release Nos. 33-10459; 34-82746. Available at: https://www.sec.gov/rules/interp/ 2018/33-10459.pdf
11- World Economic Forum. (2017). The Global Risks Report 2017: 12th Edition. Available at: http://www3.weforum.org/docs/GRR17_Report_web.pdf.