نموذج مقترح لتعزيز كفاءة التحصيل الضريبي باستخدام استراتيجيات الأمن السيبراني: دراسة تطبيقية

الشيماء فؤاد شرف*

الملخص

هدف هذا البحث إلى تقديم نموذج لتحسين كفاءة التحصيل الضريبي من خلال تطبيق استراتيجيات الأمن السيبراني، مع التركيز على الشركات المقيدة في البورصة المصرية. تم اعداد هذا النموذج استجابةً للتحديات المتزايدة التي تفرضها التهديدات السيبرانية على البيانات الضريبية وسير عمليات التحصيل.

استندت منهجية البحث إلى تحليل البيانات المستخلصة من المراجعات الأدبية والدراسات السابقة، ومقابلات مع مختصين في مجال الأمن السيبراني والتحصيل الضريبي. اعتمدت الدراسة التطبيقية على عينة مكونة من 135 شركة من الشركات المقيدة بالبورصة المصرية خلال الفترة من 2020 حتى 2023.

أظهرت نتائج البحث تأثيرًا إيجابيًا لتطبيق استراتيجيات الأمان السيبراني (مثل استخدام الجدران النارية، تشفير البيانات، وتطبيق تقنيات الكشف عن التسلل) على تعزيز كفاءة التحصيل الضريبي. كما أشارت النتائج إلى امكانية تقليل حالات التهرب الضريبي وزيادة نسبة التحصيل الفعلي من خلال تحسين سرعة وفعالية عمليات الحماية. ساعد تحسين أنظمة الحماية السيبرانية المتقدمة في الكشف المبكر عن محاولات الاحتيال، مما أدى إلى تقليل الأخطاء وزيادة دقة وسرعة عملية التحصيل.

الكلمات المفتاحية: الأمن السيبراني، كفاءة التحصيل الضريبي، التهرب الضريبي، الهجمات السيبرانية، استراتيجيات الأمن السيبراني.

* مدرس المحاسبة بالمعهد العالي للتسويق والتجارة ونظم المعلومات

Proposed Model to Enhance Tax Collection Efficiency Using Cybersecurity Strategies: An Applied Study

Abstract

This research aims to present a model to improve the efficiency of tax collection through the application of cybersecurity strategies, with a focus on companies listed on the Egyptian Stock Exchange. This model was developed in response to the growing challenges posed by cyber threats to tax data and the processes of tax collection.

The research methodology was based on an analysis of data derived from literature reviews, previous studies, and interviews with experts in the fields of cybersecurity and tax collection. The applied study relied on a sample of 135 companies listed on the Egyptian Stock Exchange during the period from 2020 to 2023. The research findings indicated a positive impact of applying cybersecurity strategies (such as the use of firewalls, data encryption, and intrusion detection technologies) on enhancing tax collection efficiency.

The results also suggested that reducing tax evasion and increasing actual tax collection rates could be achieved by improving the speed and effectiveness of protection mechanisms. Furthermore, the enhancement of advanced cybersecurity systems contributed to the early detection of fraud attempts, resulting in fewer errors and greater accuracy and speed in the tax collection process.

Keywords: Cybersecurity, Tax Collection Efficiency, Tax Evasion, Cyber Attacks, Cybersecurity Strategies.

1 القسم الأول
الإطار المنهجي للبحث

1/1 مقدمة البحث

مع التقدم التكنولوجي السريع والاعتماد المتزايد على الأنظمة الرقمية في مختلف القطاعات؛ أصبحت قضايا الأمن السيبراني تشكل تحديًا جوهريًا للمؤسسات والحكومات على حد سواء. حيث يعتمد الاقتصاد بشكل متزايد على التكنولوجيا في إدارة العمليات المالية والضريبية، وفي هذا السياق يمثل التحصيل الضريبي أحد المجالات الحيوية التي تتطلب حماية من التهديدات السيبرانية المتزايدة التي تتنوع من البرمجيات الخبيثة إلى هجمات الفدية؛ حيث تشكل تهديدًا كبيرًا للأمان والسرية والنزاهة في نظم التحصيل الضريبي. كما إن حماية البيانات الضريبية من التهديدات السيبرانية وضمان كفاءة عمليات التحصيل الضريبي يعدان من التحديات الكبرى التي تواجهها السلطات الضريبية خاصة مع تطور أساليب الجرائم الإلكترونية وازديادها تعقيدًا (***Plena S. 2024; Palil M. 2020***).

كما يعد حدوث اختراقات للأمن السيبراني من المخاطر الرئيسية التي تواجهها الشركات في العالم الرقمي، ولقد أدى الارتفاع في اختراقات الأمن السيبراني إلى جعل الأمن السيبراني مجالًا بالغ الأهمية للشركات والأسواق والجهات التنظيمية العالمية. حيث تشير بعض التقديرات إلى أن التكاليف من اختراقات الأمن السيبراني قد تجاوزت 2 تريليون دولار في عام 2019 ***(Juniper R., 2015)***، وارتفع متوسط عدد اختراقات الأمن السيبراني المبلغ عنها بنسبة 38% في عام 2015 مقارنة بما تم تسجيله في عام 2014، مع متوسط خسارة مالية قدرها 2.7 مليون دولار ***(PWC, 2016)***، وأدت اختراقات الأمن السيبراني للشركات مثل ***Equifax، Yahoo، Target*** إلى تأثيرات شديدة على أسعارها وأرباحها في السوق.

وقد كشفت دراسة ***(Asiri, M., 2022)*** عن مدى ارتباط التجنب الضريبي للشركات بحدوث اختراق للأمن السيبراني، وتضمنت ضرورة دراسة هذا الارتباط لأن عدم الإفصاح عن الاختراقات السيبرانية يؤدي إلى زيادة التكاليف وعدم تناسق المعلومات مما يساعد على ازدهار بيئة التخطيط الضريبي ***(Kim et al., 2011).***

2/1 مشكله البحث

في ظل التطور السريع للتكنولوجيا الرقمية وزيادة الاعتماد على الأنظمة الإلكترونية في مختلف القطاعات، أصبحت السلطات الضريبية تواجه تحديات كبيرة تتعلق بأمن المعلومات وحماية البيانات، وتعتبر الهجمات السيبرانية والاختراقات الإلكترونية من أكبر المخاطر التي تهدد كفاءة التحصيل الضريبي. حيث يمكن أن تؤدي إلى فقدان المعلومات أو التلاعب بها، مما يؤثر سلباً على دقة التحصيل، والشفافية، ونقص ثقة الممولين في المنظومة الضريبية وبالتالي زيادة التهرب.

حيث تعتبر مشكلة التهرب الضريبي واحدة من التحديات الرئيسية التي تواجه الحكومات في جميع أنحاء العالم، فقد تؤدي إلى خسارة الإيرادات العامة وتعرقل التنمية الاقتصادية، ومع التطور التكنولوجي وانتشار التعاملات الرقمية ظهرت فرص جديدة لمرتكبي التهرب الضريبي لاستخدام تقنيات متقدمة للإفلات من الرقابة. لذلك يتطلب الأمر تطوير استراتيجيات أمنية سيبرانية فعالة لمواجهة هذه التحديات ***(Madani, L., et al., 2024; Mulyani et al., 2023).***

وتعانى الكثير من الدول بما فيها مصر من فجوات في البنية التحتية السيبرانية المستخدمة في الأنظمة الضريبية، هذا القصور يؤدي إلى ضعف كفاءة التحصيل الضريبي ويزيد من احتمالية تعرض الأنظمة للتهديدات السيبرانية. بناءً عليه تظهر الحاجة إلى استراتيجيات قوية للأمن السيبراني لتحسين كفاءة عمليات التحصيل الضريبي وضمان حماية البيانات من أي اختراقات محتملة.

وبناءً على ما سبق تتمثل مشكلة البحث في الإجابة على هذا السؤال الرئيسي: "كيف يمكن لاستراتيجيات الأمن السيبراني أن تعزز من كفاءة التحصيل الضريبي؟" وذلك من خلال الإجابة على الأسئلة الفرعية التالية:

1. ما هي أبرز التهديدات السيبرانية التي تواجه الشركات المقيدة في البورصة المصرية والجهود المبذولة لمواجهتها؟
2. كيف يمكن اعداد استراتيجيات فعالة لمواجهة التهديدات السيبرانية؟
3. ما مدى فعالية السياسات الأمنية الحالية في حماية أنظمة التحصيل الضريبي من هذه التهديدات؟
4. كيف يمكن اعداد نموذج مقترح لتعزيز كفاءة التحصيل الضريبي باستخدام استراتيجيات الأمن السيبراني؟

3/1 أهداف البحث

يهدف البحث إلى تصميم واعداد نموذج مقترح لتعزيز كفاءة التحصيل الضريبي من خلال تطبيق استراتيجيات الأمن السيبراني يتضمن تدابير وقائية فعالة من الهجمات السيبرانية، وهناك أهداف فرعية تمثلت فيما يلي:

أ. دراسة العلاقة بين استراتيجيات الأمن السيبراني المستخدمة ومستوى كفاءة التحصيل الضريبي.

ب. فهم التهديدات والمخاطر الأمنية التي تؤثر على أنظمة التحصيل الضريبي واقتراح حلول لتقليل تلك المخاطر.

ج. تصميم نموذج يعتمد على استراتيجيات الأمن السيبراني لتحسين كفاءة الأنظمة الضريبية وضمان حماية المعلومات.

د. تقديم توصيات للجهات المسؤولة حول كيفية تطبيق استراتيجيات الأمن السيبراني بشكل فعّال في عمليات التحصيل.

4/1 أهمية البحث

تبرز أهمية البحث من خلال النقاط التالية:

أ. يسلط الضوء على أهمية استخدام التقنيات الحديثة في حماية البيانات الضريبية من الهجمات السيبرانية.

ب. تعزيز كفاءة وشفافية التحصيل الضريبي من خلال الاستفادة من استراتيجيات الأمن السيبراني، مما يُسهم في بناء ثقة المواطنين في النظام الضريبي ويؤدي إلى تقليل التهرب الضريبي.

ج. تحسين كفاءة التحصيل الضريبي يعزز من موارد الدولة ويقلل من الفاقد الضريبي، مما ينعكس إيجاباً على الاقتصاد الوطني.

5/1 فرضيات البحث

الفرضية الرئيسية: لا توجد علاقة ذات دلالة إحصائية بين استخدام استراتيجيات الأمن السيبراني وكفاءة التحصيل الضريبي، ويتفرع منه الفروض التالية:

أ. لا يوجد تأثير جوهري لاستخدام استراتيجيات الأمن السيبراني على تقليل الهجمات السيبرانية التي تستهدف أنظمة التحصيل الضريبي.

ب. لا يوجد تأثير جوهري عند تطبيق تقنيات الأمن السيبراني في تحسين شفافية العمليات الضريبية وثقة دافعي الضرائب في النظام الضريبي.

ج. لا يوجد تأثير جوهري لتطبيق نموذج الأمن السيبراني المقترح على تقليل الفاقد الضريبي وزيادة الإيرادات الضريبية.

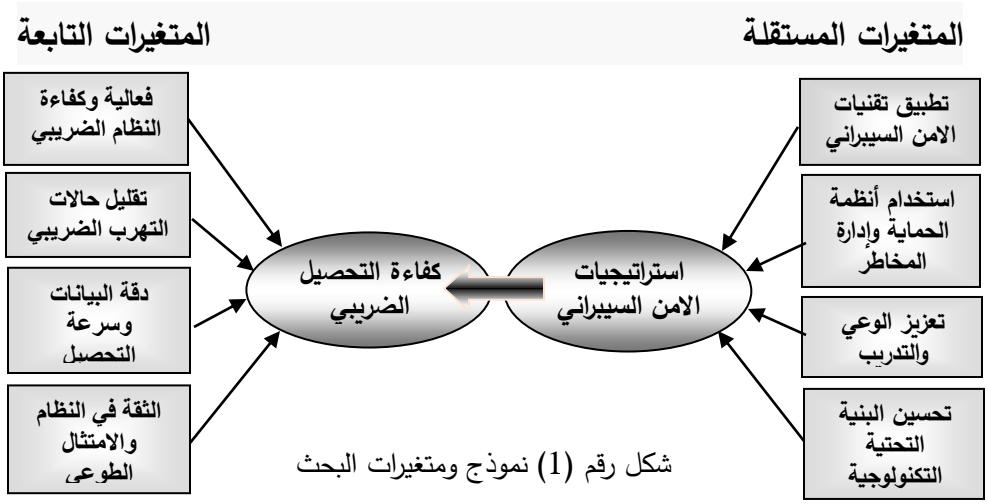
6/1 نطاق وحدود البحث

يتضمن نطاق البحث تحليل استراتيجيات الحماية السيبرانية المستخدمة حاليًا وتقييم مدى فعاليتها في مواجهة التهديدات السيبرانية التي تواجه أنظمة التحصيل الضريبي. كما يشمل تصميم نموذج مقترح لتعزيز كفاءة التحصيل الضريبي عبر تطبيق تقنيات الحماية السيبرانية المتقدمة. وتشمل حدود البحث:

1. حدود مكانية: يركز البحث على الشركات المقيدة في البورصة المصرية، ويستهدف عينة مكونة من 135 شركة.
2. حدود زمانية: يغطي البحث الفترة من 2020 إلى 2023.

7/1 نموذج ومتغيرات البحث

يهدف النموذج إلى تعزيز كفاءة التحصيل الضريبي باستخدام استراتيجيات الامن السيبراني، ويوضح الشكل التالي رقم (1) متغيرات البحث كما يلي:



شكل رقم (1) نموذج ومتغيرات البحث

8/1 منهجية البحث

يعتمد البحث على المنهج الوصفي التحليلي. حيث يتم تحليل استراتيجيات الأمن السيبراني المستخدمة في الأنظمة الضريبية وتقييم مدى تأثيرها على كفاءة التحصيل الضريبي. كما يتم استخدام المنهج التطبيقي من خلال اختبار النموذج المقترح على عينة من الشركات المقيدة في البورصة المصرية لتقييم فاعليته.

يجمع البحث البيانات من مصادر متعددة مثل الدراسات السابقة، الوثائق الحكومية، والمقابلات مع خبراء في المجال الضريبي والسيبراني، بالإضافة إلى استخدام تقنيات تحليل البيانات لتقديم استنتاجات وتوصيات.

9/1 الدراسات السابقة

تعددت الدراسات التي تناولت أثر الأمن السيبراني على الجوانب المحاسبية والضريبية وجودة المراجعة، وفيما يلي بعض هذه الدراسات الهامة:

أ- دراسة *(Madani, L., et al., 2024)*:

هدفت هذه الدراسة إلى معرفة تأثير الإفصاح عن الأمن السيبراني والمخاطر الضريبية والسمعة وخبرة المراجع على جودة المراجعة، وتوصلت الدراسة إلى أن كل من الإفصاح عن الأمن السيبراني، المخاطر الضريبية، سمعة المراجع، وخبرة المراجع لهم تأثير سلبي على جودة المراجعة.

ب- دراسة *(Hossain & Johora, 2024)*:

هدفت هذه الدراسة إلى تقديم تحليل شامل لكيفية تشكيل الأمن السيبراني لمهنة المحاسبة في العصر الرقمي، وتسليط الضوء على الفرص والتحديات المقبلة، واستكشاف الدور الحاسم للأمن السيبراني في حماية البيانات المالية في مهنة المحاسبة، وتوصلت الدراسة إلى فعالية استراتيجيات الأمن السيبراني متعددة الطبقات في تعزيز أمن البيانات، والحد من الانتهاكات، وتحسين قدرات الكشف عن الاحتيال.

ج- دراسة *(Mulyani, S., et al., 2023)*:

هدفت الدراسة إلى إنشاء إطار شامل لضرائب التجارة الإلكترونية. حيث يتناول الجوانب الحاسمة للتنمية الاقتصادية والعدالة في الاقتصاد الرقمي من خلال تحسين آليات تحصيل الضرائب، وتوصلت الدراسة إلى توفير أساس قوي لتحسين اللوائح الضريبية الحالية للتجارة الإلكترونية، ودعم النمو المستدام للاقتصاد الرقمي في إندونيسيا، وتطوير السياسات الضريبية العادلة والفعالة في المجال الرقمي، وبالتالي تعزيز التنمية الاقتصادية وتعزيز القدرة التنافسية للدولة.

د- دراسة *(Krivokapic et al., 2023)*:

هدفت هذه الدراسة إلى معالجة الجانب القانوني والمنفعة الاقتصادية لدفع الفدية، إلى جانب تغطية التكاليف الإضافية المتعلقة باسترداد الأداء التجاري للكيان المهاجم قبل الهجوم، وتحليل الآثار المالية للهجمات، ودوافع الضحية لدفع الفدية، والآثار القانونية والمحاسبية والضريبية لمثل هذا الدفع، وتوصلت الدراسة إلى أن دفع الفدية غير قانوني، ويمكن التعامل معه على أنه دفع مستحقات، نفقات رأسمالية، وسرقة، ومع ذلك لا يمكن الاعتراف بالمدفوعات لأغراض إعداد التقارير المالية أو الضريبية، وبالتالي فهي تخضع لعدد من الضرائب.

هـ- دراسة *(Kayode, O., et al., 2022)*:

هدفت الدراسة إلى تناول التهرب الضريبي المتعلق باستراتيجيات تخفيف آثار غسل الأموال القائمة على التجارة في نيجيريا في عصر الأمن السيبراني، وتوصلت الدراسة إلى أن نمو الاقتصاد النيجيري سوف يتباطأ مع زيادة غسيل الأموال. كما أشارت نتائج الدراسة إلى أن من بين واجبات البنوك في التعرف على عمليات الاحتيال عبر الإنترنت هو تطوير رقم التحقق البنكي، ونظام حساب الخزينة الموحد، وتعليمات محصل الضرائب.

و- دراسة *(Asiri, M., 2022)*:

هدفت هذه الدراسة إلى تقديم ثلاث مقالات تدرس العلاقة بين تجنب الضرائب على الشركات وكفاءة الاستثمار، تعقيد إعداد التقارير المحاسبية واختراقات الأمن السيبراني، وأخيرًا حدوث اختراقات الأمن السيبراني والتهرب الضريبي للشركات، وتوصلت الدراسة إلى وجود علاقة إيجابية وذات دلالة إحصائية بين حدوث اختراقات الأمن السيبراني وتجنب ضرائب الشركات، وأن الشركات التي لديها حوكمة تقنية المعلومات أقل احتمالاً للانخراط في تجنب ضرائب الشركات.

- **تحليل وتقييم الدراسات السابقة وتحديد الفجوة البحثية:**

أظهرت الدراسات السابقة تنوعاً في تناول موضوع الأمن السيبراني وتأثيراته على المجالات المالية والضريبية. فقد تناولت بعض الدراسات تأثير الإفصاح عن الأمن السيبراني والمخاطر الضريبية على جودة المراجعة. بينما ركزت بعضها على فعالية استراتيجيات الأمن السيبراني في حماية البيانات المالية والحد من الاحتيال في مهنة المحاسبة، وهناك من كان معنيًا بتحسين آليات تحصيل الضرائب في التجارة الإلكترونية لتعزيز التنمية الاقتصادية. أو بحث العلاقة بين اختراقات الأمن السيبراني وتجنب الشركات للضرائب.

وعلى الرغم من تعدد الدراسات التي تناولت تأثير الأمن السيبراني على الجوانب المالية والضريبية، إلا أن هناك فجوة في الأبحاث المتعلقة بتطبيق استراتيجيات الأمن السيبراني لتحسين كفاءة التحصيل الضريبي بشكل مباشر، وخاصة في سياق الأنظمة الضريبية في مصر. هذه الفجوة تتطلب دراسات معمقة تستكشف كيفية الاستفادة من التقنيات السيبرانية لتعزيز كفاءة وشفافية عمليات التحصيل الضريبي.

10/1 تنظيم البحث

لتحقيق أهداف البحث واختبار فروضه تم تقسيمه إلى خمسة أقسام وذلك كما يلي:

القسم الأول: الإطار المنهجي للبحث.

القسم الثاني: التحديات السيبرانية التي تواجه الأنظمة الضريبية.

القسم الثالث: تأثير استراتيجيات الأمن السيبراني على كفاءة التحصيل الضريبي.

القسم الرابع: نموذج مقترح لتحسين كفاءة التحصيل الضريبي باستخدام الامن السيبراني.

القسم الخامس: الدراسة التطبيقية وتقييم الفروض.

وينتهي البحث بالنتائج والتوجهات البحثية المستقبلية.

2 القسم الثاني
تحديات الأمن السيبراني التي تواجه الأنظمة الضريبية

1/2 مقدمة

إن ضمان الأمن السيبراني ليس مهمة سهلة وإنما تتطلب معرفة في المجال وقدرات لتحديد التهديدات المحتملة عبر بيانات الشبكة ***(السرحان، 2020)***. كما تواجه الأنظمة الضريبية تحديات كبيرة في مجال الأمن السيبراني بسبب تزايد التهديدات الرقمية والتعقيد المتزايد في الهجمات الإلكترونية، وتشمل هذه التحديات حماية البيانات الحساسة للمكلفين وضمان استمرارية العمليات الضريبية دون انقطاع أو تعرض للاختراق.

2/2 مفهوم الأمن السيبراني

الأمن السيبراني ***Cyber Security*** هو عملية الهدف منها حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات، وما تحتويه من بيانات من أي اختراق أو تعطيل أو تعديل، أو دخول أو استخدام أو استغلال غير مشروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ***(آل سعود، 2024)***.

ويعرف بأنه عبارة عن مجموعة من التقنيات والعمليات والممارسات التي تحمى وتضمن حماية أصول المنشأة ***(Vasarhelyi, 2017)***. كما يعرف الأمن السيبراني بأنه تنظيم وجمع الموارد والعمليات والهياكل التي يتم استخدامها لحماية الفضاء الإلكتروني والأنظمة الأخرى التي تدعم الفضاء الإلكتروني من الهجمات والحوادث الإلكترونية ***(علي، 2022)***.

وأكدت منظمة المعايير الدولية ***(ISO, 2016)*** أن الأمن السيبراني يتمثل في المحافظة على السرية والنزاهة وتوافر المعلومات في الفضاء السيبراني.

3/2 أهداف الأمن السيبراني

تتمثل الأهداف العامة للأمن السيبراني (***Cybersecurity***) في الحفاظ على سرية المعلومات وسلامتها وتوافرها ***(علي، 2022)***. **كما** تسعى الدول ومنظمات الأعمال حول العالم إلى تعزيز الأمن السيبراني، وذلك لتحقيق العديد من الأهداف، والتي يمكن إيضاحها على النحو الآتي ***(الصائغ، 2018)***:

1- العمل على توفير بيئة آمنة تتسم بقدر كبير من الموثوقية.
2- تعزيز حماية أنظمة التقنيات التشغيلية ومكوناتها، سواء أجهزة أم برمجيات، وما تحتويه من بيانات.
3- التصدي لحوادث أمن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.
4- توفير متطلبات الحماية للحد من الجرائم السيبرانية ***(علي، 2023)***.
5- التصدي للبرمجيات الخبيثة، وما تستهدفه من إحداث أضرار بالمستخدمين، وأنظمة المعلومات.
6- الحد من التخريب والتجسس الإلكتروني بالنسبة للحكومات والأفراد.
7- سد الثغرات التي تحدث نتيجة نقاط ضعف أنظمة الحاسوب وأنظمة المعلومات.

4/2 مخاطر الأمن السيبراني

عُرفت بأنها مجموعة المخاطر التنظيمية والتشغيلية والتكنولوجية التي تتعرض لها منظمات الأعمال المعتمدة على تقنيات تكنولوجيا المعلومات الحديثة، والتي قد تحدث نتيجة اختراق نظام الأمن السيبراني لديها، بما يحد من القدرة على تحقيق الأهداف المرجوة ***(علي، 2023)***.

وتتعدد مخاطر الأمن السيبراني. فمنها المخاطر التكنولوجية والتشغيلية والتنظيمية الناتجة عن اختراق النظام ***(Badawy, 2021)*** ومخاطر الأداء التي تعبر عن فشل الأدوات التقنية في تحقيق أهدافها، ومخاطر الاختراق المادي والتجسس

الموجي عن بعد، والمخاطر المرتبطة بالعاملين نتيجة استغلال العلاقات الاجتماعية للوصول غير المرخص به ***(أحمد، 2023)***.

وعلي الرغم من وجود مزايا رائعة لاستغلال التقدم في تكنولوجيا المعلومات، إلا أنها يرافقها عالم متغير من المخاطر والتهديدات والهجمات السيبرانية غير المسبوقة ***(شرف، 2023)***، والتي يتم اعتبارها أكثر المخاطر إثارة للقلق لكل شركة في العالم ***(SEC, 2018; Gao et al. 2020)***، والأكثر سوءً واحتمالًا بعد الكوارث الطبيعية وينظر إلى تهديدات الأمن السيبراني كأهم التحديات التي تواجهها الشركات، وتمثل تهديدًا خطيرًا وتؤثر سلباً علي نموها المستقبلي، لعدة أسباب أهمها فقدان الملكية الفكرية، تعطيل العمليات، سرقة الأسرار التجارية، اضطرابات الأعمال، الإضرار بالسمعة، فقدان ثقة أصحاب المصالح، وتدهور أداء الأسهم وقيمة الاستثمارات ***(Ali et al 2021; Barry et al., 2022)***.

4/2 التهديدات السيبرانية وضوابط الحماية

تشمل التهديدات في الأمن السيبراني أنواع متعددة أهمها ***(آل سعود، 2024)***: (البرمجيات الخبيثة، حصان طروادة، التصيد للمعلومات، التسلسل المتقدم طويل الأجل، الدودة الخبيثة، فيروس الفدية الخبيث، استغلال البرامج الثنائية، التصيد المباشر، هجمات رفض الخدمة)، وفيما يلي توضيح للتهديدات وضوابط الحماية:

1/4/2 أنواع الهجمات في الأمن السيبراني

يمكن توضيح بعض الهجمات السيبرانية كما يلي:

أ- سرقة كلمات المرور: إن استخدام كلمة المرور للدخول إلى معلومات غير مخولة يتم بعدة طرق، منها التخمين فقد يستخدم الشخص المستهدف إما أسمه، أو تاريخ ميلاده، أو أي رموز معينه يسهل اكتشافها. أو عن طريق التلصص والخداع ***(شلوش، 2018)***.

بـ- هجمات رفض اداء الخدمة: يتم عن طريق محاولة تعطيل النظام لمنع المستخدمين من الوصول إلى الخدمات. فيقوم المخترق بتحميل النظام المستهدف بكمية من الطلبات التي تفوق طاقته التحميلية مما يؤدي إلى انهيار النظام ويصبح غير متاح للخدمة ***(الصباحي، 2017)***.

جـ- هجمات التصيد الاحتيالي: يتم عن طريق استبدال صفحة الويب للشخص المستهدف بصفحة ويب أخرى شبيهه، واجباره الإفصاح عن معلومات مهمة مثل معلومات بطاقة الائتمان وكلمات السر ***(خالد، 2013)***.

دـ- الهجمات الخداعية: يستغل هذا النوع من الهجمات أوجه القصور في بروتوكولات الاستقبال والإرسال لمحاولة التسلل إلى النظام. حيث إن آلية عمل معظم البروتوكولات تعتبر من المعلومات العامة التي يسهل على الجميع معرفتها، فتشمل الهجمات إعادة توجيه الرسائل أو منع إرسالها.

هـ- الهجمات على البنية التحتية الحرجة: وتستهدف هذه الهجمات البنية التحتية للنظام من شبكات اتصالات وصرافة، فكلما كانت البنية التحتية مرتبطة بالإنترنت كان تأثير هذه الهجمات أقوى على النظام ***(اللواتي، 2017)***.

كما أشار البعض ***(موسى، 2023)*** ثلاث أنواع من الهجمات السيبرانية وهي:

أ – هجمات بوابة الدخول إلى الانترنت ***Gateway Attacks***

تعد من الأساليب التي تستخدمها الشركة في الدخول إلى الانترنت وتعتبر، ويوجد نوعين من الهجمات: **الأول** وهي هجمات تشويه الموقع الالكتروني والتي يقوم فيها المهاجم بتشوية الموقع الالكتروني للشركة، بحيث يعرض الموقع الالكتروني محتوى مختلف عن المحتوى الأساسي له، ويتمثل **الثاني** في هجمات رفض تقديم الخدمة، وفيها يعمل المهاجم على عدم اتاحة الموقع الالكتروني أو خادم البريد الالكتروني للاستخدام من قبل الأفراد المستخدمين لهم.

ب – هجمات أنظمة المعلومات:

تتطلب هذه الهجمات الدخول إلى الأنظمة الداخلية للشركة من خلال استخدام العاملين، وفيه يقوم المهاجم باستخدام أسلوب ***Phising*** لتغويه واقناع أحد العاملين غير المعروفين بتنزيل وتحميل ***Malware*** والتي تسمح للمهاجم الوصول إلى جهاز الحاسب الإلى والشبكة الخاصة بالعاملين، ومن خلال ذلك يستطيع أن يرتكب هجمات أخرى أكثر حدة على الخوادم الداخلية للمنظمة وشبكات قواعد البيانات.

ج – هجمات الأنظمة التشغيلية:

وفيها يستطيع المهاجم ليس فقط الوصول إلى الأنظمة الداخلية للشركة، وإنما يستطيع التعرف أيضاً على نقاط الضعف في الأنظمة المستخدمة من قبل الشركة، وينتج عنها أضرار جسيمة للشركة.

2/4/2 ضوابط الحماية للأمن السيبرانية

الحماية من التهديدات الداخلية الناتجة عن انخفاض وعي الموظفين. حيث تبين أنها أخطر التهديدات ***(Alqahtani, 2017)*** والحماية من التهديدات الخارجية من خلال بناء جدار حماية يعمل على مدار الساعة كمرشح إلكتروني لتصفية المخاطر الرقمية الخارجية، ومعالجة ثغرات النظام ***(Ki-Aries & Faily, 2017)***، وتحقيق رؤية شاملة على نقاط القوة والضعف والثغرات التكنولوجية المحتملة التي تؤثر على تقييم الأداء المالي، والعمل على حلها بأسرع وقت، وتقديم مقترحات تمنع تكرارها ***(Kejwang, 2022)***.

وعلى المؤسسة توفير ضوابط الحماية لجميع مكونات بيئة تكنولوجيا المعلومات والاتصالات مثل الأنظمة والبرمجيات والشبكات والأجهزة الشبكية الموجودة لديها من أي حدث سيبراني ***(الهلسة، 2021)***:

- ايجاد نقاط فصل للشبكات بما يضمن عزل تأثير الأنظمة المعرضة للاختراق السيبراني عن غيرها في حال حدوث هجمات سيبرانية.

- إجراء عمليات الفحص والتجريب ضمن بيئة امنة منفصلة عن البيئة الفعلية.
- تقييم كفاءة أجهزة الحماية باستمرار لتلبية احتياجات العمل.
- الاحتفاظ بقائمة محدثة للأجهزة المتصلة بشبكة الشركة ومخططات مركز معلومات المواقع الرئيسية وموقع التعافي من الكوارث للشركة بمكان آمن.
- حصر عمليات وصول الموظفين للإنترنت بالمواقع الموثوقة من خلال استخدام برمجيات ***Firewall***.
- توفير الأنظمة اللازمة لمراقبة أمن البنية الرقمية وتحذير وكشف الاختراق الإلكتروني وبرامج الحماية من الفيروسات والتأكد من تحديثها بشكل مستمر.

3/4/2 دراسة حالات عملية للحماية السيبرانية

تقوم الباحثة من خلال الجدول رقم (1) بعرض بعض الحالات العملية لبعض شركات المحاسبة الرائدة في العالم لمواجهة الاختراق السيبراني للمعلومات كما يلي:

جدول رقم (1) حالات عملية لمواجهة الاختراقات السيبرانية

أسم الشركة	الإجراءات المتخذة للحماية	مكونات إطار عمل الأمن السيبراني
ديلويت ***(Deloitte, 2020)***	نفذت تدابير شاملة للأمن السيبراني لحماية بياناتها المالية، وتستخدم نهجًا أمنيًا متعدد الطبقات يوفر التشفير المتقدم والمراقبة المستمرة وقدرات التعرف على التهديدات. تم تصميم استراتيجية الأمن السيبراني للشركة لتحديد المخاطر والتخفيف من التهديدات المحتملة قبل أن تتمكن من التأثير على العمليات، وتستفيد الشركة من الذكاء الاصطناعي والتعلم الآلي لتعزيز أنظمة الكشف عن الاحتيال	- التشفير المتقدم: استخدام التشفير الشامل لحماية البيانات أثناء الراحة وأثناء النقل. - المراقبة المستمرة: تنفيذ أنظمة مراقبة في الوقت الفعلي لاكتشاف التهديدات والاستجابة لها على الفور. - استخبارات التهديد: استخدام الذكاء الاصطناعي ***AI*** والتعلم الآلي لتحليل بيانات التهديد والتنبؤ بالهجمات المحتملة

إسم الشركة	الإجراءات المتخذة للحماية	مكونات إطار عمل الأمن السيبراني
برايس وترهاوس كوبرز ***(PwC, 2021)***	قامت بتطوير إطار عمل قوي للأمن السيبراني يركز على الإدارة الاستباقية للتهديدات والامتثال لمعايير الأمان العالمية، ويتم دمج تدابير الأمن السيبراني للشركة في عملياتها المحاسبية، مما يوفر بيئة آمنة للتعامل مع البيانات المالية الحساسة، وتتضمن استراتيجية الشركة تقنيات متقدمة وشراكات استراتيجية لتعزيز وضعها الأمني.	- الإدارة الاستباقية للتهديدات: نشر أدوات الكشف عن التهديدات المتقدمة لتحديد المخاطر وتخفيفها قبل حدوثها. - الامتثال للمعايير العالمية: الالتزام بمعايير الأمن السيبراني الدولية مثل ***ISO/IEC 27001.*** - الشراكات الإستراتيجية: التعاون مع شركات الأمن السيبراني الرائدة للبقاء في صدارة التهديدات الناشئة.
إرنست ويونغ ***(EY, 2019).***	نفذت استراتيجية شاملة للأمن السيبراني تركز على حماية بيانات العملاء وضمان سلامة عملياتها المحاسبية. يتضمن نهج الشركة الاستفادة من تقنية ***blockchain*** لتعزيز أمن وشفافية الخدمات المالية. تستخدم الشركة أيضًا التحليلات المتقدمة والذكاء الاصطناعي AI لرصد وتحليل حركة مرور الشبكة، وتحديد أنشطة الاختراق في الوقت الفعلي.	- تقنية ***Blockchain***: تقوم هذه التقنية بإنشاء دفتر أستاذ آمن ومقاوم للتلاعب للمعاملات المالية. - التحليلات المتقدمة: تطبيقات التعلم الآلي للكشف عن الانتهاكات الأمنية المحتملة. - تدريب الموظفين: برامج تدريب مستمرة لإبقاء الموظفين على الاطلاع بأحدث تهديدات الأمن السيبراني وأفضل الممارسات. - يساعد تركيز شركة ***EY*** على التقنيات المبتكرة والتحسين المستمر على البقاء في مجال المحاسبة.

المصدر: اعداد الباحثة

5/2 تحديات الأمن السيبراني للسلطات الضريبية

1/5/2 السلطات الضريبية كهدف رئيسي للهجمات الإلكترونية

تلعب السلطات الضريبية أدوارًا بالغة الأهمية في الأنظمة المالية الوطنية مما يجعلها أهدافًا رئيسية للهجمات الإلكترونية. حيث تدير مبالغ ضخمة من الأموال والمعلومات الحساسة وتلعب دورًا حاسمًا في النشاط التشغيلي للخدمات الحكومية، وقد تعتمد السلطات الضريبية على أنظمة تكنولوجيا المعلومات القديمة، مما يزيد من تعرضها للتهديدات الرقمية، وبصرف النظر عن الأضرار التشغيلية والمالية التي يمكن أن تلحقها الهجمات الإلكترونية بالسلطات الضريبية، فإن تعطيل السلطات الضريبية يُنظر إليه على أنه إنجازات للمهاجمين الإلكترونيين ***(Plena S., 2024)***.

2/5/2 الأهداف الرئيسية للهجمات الإلكترونية على السلطات الضريبية

تشكل السلطات الضريبية جزءًا أساسيًا من أي بنية تحتية اقتصادية وطنية وهي أهداف مربحة للمهاجمين الإلكترونيين نظرًا للأصول التي تمتلكها، وتشمل بعض العوامل التي تجعل السلطات الضريبية أهدافًا جذابة للهجمات ما يلي:

1/2/5/2 الدور الاستراتيجي للسلطات الضريبية في الاقتصادات الوطنية: تعتبر السلطات الضريبية مصدرًا بالغ الأهمية لتمويل الخدمات العامة، فهي تتعامل مع المعاملات المالية المهمة وتؤثر على السياسات المالية. إن تأثير الهجوم على السلطات الضريبية يتجاوز الخسارة المالية الفورية. فهو يؤثر على خصوصية الأفراد وتعطيل الاستقرار المالي، وإلحاق الضرر بالثقة العامة، والإضرار بسمعة السلطة ***(Krivokapic et al., 2023)***.

2/2/5/2 تحتفظ السلطات الضريبية بكم هائل من البيانات الحساسة: تعتبر السلطات الضريبية أهدافًا رئيسية لمجرمي الإنترنت لأنها تخزن كميات كبيرة من المعلومات الحساسة، ويشمل ذلك البيانات الشخصية والمالية للأفراد والشركات،

وإذا سُرقت هذه البيانات، فقد يؤدي ذلك إلى مشاكل خطيرة مثل سرقة الهوية والاحتيال المالي وقد يؤثر سلبًا على التعاون الدولي في مجال المعلومات.

3/2/5/2 الأنظمة المعلوماتية المعرضة للخطر: في كثير من الحالات تكون الأنظمة التي تستخدمها السلطات الضريبية أنظمة رقمية قديمة، مما يجعلها معرضة للخطر في نقاط متعددة، ويسعى مجرمو الإنترنت إلى استغلال هذه الثغرات لشن هجمات معقدة ***(Mulyani et al., 2023)***.

3/5/2 أمثلة على الهجمات الإلكترونية على السلطات الضريبية

1/3/5/2 هجوم ***DDoS*** على مصلحة الضرائب البولندية، مارس 2023:

أ. نوع الهجوم: هجوم الحرمان من الخدمة الموزعة (*DDoS*)، مما يتسبب في تعطيل البوابة الضريبية الوطنية البولندية.

ب. التأثير: اضطراب قصير المدى، مع تعطل الموقع الإلكتروني وحظر الوصول إلى الضرائب عبر الإنترنت ليوم واحد.

ج. الحل: لم يحدث أي خرق للبيانات، حيث قامت السلطات بمراقبة وإدارة الحادث دون تحديد تفاصيل إضافية للاسترداد.

2/3/5/2 هجوم برامج الفدية على الأنظمة الحكومية كوستاريكا، مايو 2022

أ. نوع الهجوم: هجوم فدية من قبل مجموعة كونتي، باستخدام البرمجيات الخبيثة لتشفير أنظمة الحكومة، والمطالبة بفدية قدرها 20 مليون دولار.

ب. التأثير: حدوث اضطرابات شديدة في الخدمات الحكومية، وكذا تحصيل الضرائب والجمارك، مما أثر على اقتصاد كوستاريكا وعمليات القطاع العام.

ج. القرار: رفضت حكومة كوستاريكا دفع الفدية، وبدأت جهود الاسترداد بمساعدة دولية في مجال الأمن السيبراني.

3/3/5/2 الهجوم على مصلحة الضرائب الأمريكية (*IRS*) المخترق في هجوم سلسلة توريد – *SolarWinds* ديسمبر 2020.

أ. نوع الهجوم: تعرضت مصلحة الضرائب الأمريكية لهجوم من سلسلة التوريد بإدخال رمز خبيث في برنامج مراقبة تكنولوجيا المعلومات ***المسمى Orion***، والذي برمجته شركة ***SolarWinds*** ينشئ الرمز الخبيث بابًا خلفيًا يمكن للمتسللين من خلاله الوصول للمستخدمين وحسابات المنظمات وانتحال هوياتهم. كما يمكن للبرامج الضارة الوصول لملفات النظام دون اكتشافه.

ب. التأثير: من المحتمل أن يؤدي الهجوم إلى كشف معلومات حساسة لدافعي الضرائب وتعريض سلامة البيانات الحكومية للخطر، وقد أثار ذلك مخاوف بشأن مدى قدرة المهاجمين على الوصول إلى الأنظمة الفيدرالية.

ج.الحل: بعد أن كشفت شركة ***FireEye*** عن الهجوم، قامت فرق الأمن السيبراني وتكنولوجيا المعلومات التابعة لمصلحة الضرائب بعزل برنامج ***Orion*** المخترق، وفرض تدابير أمنية صارمة إضافية ***(Mulyani et al., 2023)***.

4/5/2 التوصيات الموجهة للسلطات الضريبية لتعزيز الأمن السيبراني:

1/4/5/2 التدريب والتوعية المنتظمة: إجراء تدريب منتظم على الأمن السيبراني لجميع الموظفين، مع التركيز على مخاطر هجمات التصيد الاحتيالي وأهمية سياسات كلمات المرور القوية، وتثقيف الموظفين حول التعرف على رسائل البريد الإلكتروني المشبوهة والبروتوكولات للإبلاغ عنها ***(Kamilah & Khan, 2021)***.

2/4/5/2 التحكم في الوصول والحماية من التهديدات الداخلية: فحص الموظفين، تقسيم البيانات، تنفيذ أنظمة الكشف المبكر، وسياسات عدم الثقة، استخدام المصادقة متعددة العوامل والتأكد من أن الوصول إلى البيانات الحساسة يتم فقط على أساس الحاجة إلى المعرفة، ومراجعة امتيازات الوصول بانتظام.

3/4/5/2 الاطلاع بالتحديثات الأمنية وتحديث البنية الأساسية لتكنولوجيا المعلومات: حافظ على روتين تحديث وتصحيح جميع البرامج والأنظمة، استخدم نظامًا قويًا لمراقبة التحديثات الأمنية ونشرها للدفاع ضد الثغرات الأمنية المعروفة.

4/4/5/2 الاستفادة من إدارة استخبارات التهديدات السيبرانية: تنفيذ إدارة التعرض المستمر للتهديدات السيبرانية والاستفادة من معلومات استخبارات التهديدات السيبرانية لتحديد التهديدات الناشئة والاستجابة لها بشكل استباقي، ومن خلال النظر إلى الشبكة الداخلية من منظور المهاجمين ***(Hossain & Johora, 2024).***

5/4/5/2 تنفيذ أدوات لتقييم نقاط ضعف الأمن السيبراني بشكل مستمر: تقييمات الأمن السيبراني ليست كافية مع سرعة الهجمات وانتشار المخاطر حتى إذا قمت بإجراء تقييم في يوم واحد، ويمكن مهاجمة الأنظمة في اليوم التالي .

6/4/5/2 خطة الاستجابة للحوادث: تطوير وتحديث خطة شاملة للاستجابة للحوادث بشكل منتظم، والتأكد من أن جميع الموظفين على دراية بأدوارهم في حالة وقوع حادث إلكتروني وإجراء تدريبات منتظمة لاختبار فعالية الخطة.

6/2 الجهود المبذولة لمواجهة التحديات السيبرانية

1/6/2 الجهود الدولية للتصدي للهجمات السيبرانية

على الرغم من غياب سلطة عليا تنظم التفاعلات بالفضاء السيبراني، ولكن هناك جهود دولية تستهدف ضبط التفاعلات وسلوك الوحدات الدولية الفاعلة في الفضاء السيبراني في إطار التنظيمات الدولية القائمة ومنها ما أسفر عن اتفاقات دولية على الصعيد الإقليمي أو الثنائي بين الوحدات الدولية وبعضها البعض.

منها ما يدور حول المساعدة في وضع وصياغة الخطط والاستراتيجيات الوطنية ومنها ما يسعى لتقديم الدعم التقني والفني، ومنها ما يقدم القوي البشرية ويستهدف تدريب الكوادر، ومن أبرز الجهود الدولية بداخل التنظيمات الدولية القائمة جهود الأمم المتحدة ***(جمال الدين، 2023).*** حيث قامت بعدد من الجهود والتصدي للهجمات

والجرائم السيبرانية تنوعت بين وضع قواعد موضوعية واجرائية ومؤتمرات وقمم دولية وجهود لبعض الهيئات والاجهزة التابعة لها، فقد وضعت الأمم المتحدة مجموعة من القواعد الموضوعية والإجرائية لمواجهة الجرائم السيبرانية.

ويُلاحظ أحد الباحثين ***(عيسى، 2022)*** **تزايد اهتمام المنظمات المهنية** في الدول المتقدمة بالإفصاح عن مخاطر الأمن السيبراني، وصدور العديد من الإرشادات والتوصيات لدعم هذا الإفصاح. كما يُلاحظ عدم وجود توجه صريح في معايير المحاسبة الدولية لدعم الإفصاح عن مخاطر الأمن السيبراني، وما زالت تتم عمليات الإفصاح في ضوء القواعد الحالية كجزء من الإفصاح المالي عند الإفصاح عن خسائر الحوادث السيبرانية أو في إطار الإفصاح الاختياري.

2/6/2 أهم الجهود المصرية في دعم الأمن السيبراني

أصدرت مصر الاستراتيجية الوطنية للأمن السيبراني (٢٠١٧ – ٢٠٢١) تتضمن الاستراتيجية عددا من البرامج التي تدعم الأهداف الاستراتيجية للأمن السيبراني ***(يعقوب، 2022)***. حيث تكاثفت الجهود المصرية خلال الفترة الأخيرة لمواكبة التطورات الحادثة في مجال تكنولوجيا المعلومات وما يتبعها من مخاطر أصبحت بالفعل تؤثر على أمن واستمرار الشركات. حيث نصت المادة (٣١) من الدستور المصري المعدل في يناير (٢٠١٤) على أن "أمن الفضاء المعلوماتي جزء أساسي من منظومة الأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذي ينظمه القانون" ***(يوسف، 2022)***.

ولقد صدرت هذه الاستراتيجية عن المجلس الأعلى للأمن السيبراني، وتهدف إلى دعم الشركات في مواجهة المخاطر السيبرانية وتعزيز الثقة في البنية الاساسية للاتصالات والمعلومات وتطبيقاتها وخدماتها في جميع القطاعات الحيوية وتأمينها، وذلك لتوفير بيئة رقمية أمنة وموثوقة للمجتمع المصري ***(فريد، 2022)***.

وبناء على ذلك تم وضع **الإستراتيجية الوطنية للأمن السيبراني** ضمن رؤية الدولة المصرية (٢٠٣٠)، وقد حددت الاستراتيجية عدة برامج لتحقيق الأمن السيبراني كما يلي: ***(المجلس الأعلى للأمن السيبراني، ٢٠١٨)***

1- التحديات والأخطار السيبرانية والتي تتمثل في خطر اختراق البنية التحتية للاتصالات وتكنولوجيا المعلومات وخطر الإرهاب والحرب السيبرانية وخطر سرقة الهوية الرقمية والبيانات الخاصة.

2- أهم القطاعات الحيوية المستهدفة وتشمل على الترتيب: (القطاع الأمني، قطاع الاتصالات وتكنولوجيا المعلومات، قطاع الطاقة وقطاع الخدمات الحكومية ومنها التحصيل الضريبي، قطاع النقل، قطاع الصحة، قطاع الإعلام والثقافة).

3- العناصر الرئيسية لخطورة التهديدات السيبرانية تكمن في استنادها إلى تقنيات متقدمة ومتطورة، وأنها ذات سرعة في الانتشار، وأنها ذات نطاق واسع للتأثير.

4- قامت مصر بتأسيس "المجلس الأعلى للأمن السيبراني" وهو مسؤولاً عن الاستجابة لحوادث أمن الحاسوب والمعلومات، وتوفير الدعم والدفاع والتحليل في مجال الهجمات السيبرانية والتعاون مع الهيئات الحكومية والمالية، وتوفير الإنذار المبكر ضد انتشار البرمجيات الخبيثة والهجمات السيبرانية الضخمة.

5- التوجه الاستراتيجي لمواجهة الأخطار السيبرانية: من خلال الدعم السياسي والمؤسسي الاستراتيجي والتنفيذي، البحث العلمي والتطوير وتنمية صناعة الأمن السيبراني، تنمية الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني ***(الرشيدي، 2019)***.

6- اصدار قانون مكافحة جرائم تقنية المعلومات المعروف بمكافحة جرائم الانترنت.

وترى الباحثة أهمية اصدار معيار محاسبي مصري لوضع قواعد خاصة للإفصاح عن مخاطر الأمن السيبراني بما يساهم في توفير معلومات مفيدة لمتخذي القرارات، ويساهم في تحسين فعالية إدارة مخاطر الأمن السيبراني لدى المنشآت.

3 القسم الثالث

تأثير استراتيجيات الأمن السيبراني على كفاءة التحصيل الضريبي

1/3 مقدمة

بناءً على تحديات الأمن السيبراني السابق ذكرها التي تواجهها الأنظمة الضريبية وتهدد كفاءتها، يأتي دور استراتيجيات الأمن السيبراني في التصدي لهذه التحديات لضمان حماية البيانات وتحسين كفاءة التحصيل الضريبي. حيث تلعب استراتيجيات الأمن السيبراني دورًا حاسمًا في تحسين كفاءة التحصيل الضريبي من خلال حماية الأنظمة الضريبية من الاختراقات وضمان سلامة البيانات المالية.

2/3 الأهداف الاستراتيجية للأمن السيبراني

مع تطبيق المؤسسات الحكومية نظم التحول الرقمي أصبح من الضروري تدعيم وتحقيق الأمن السيبراني مما يتطلب تطوير النظم المتبعة على مستوى الجهاز الحكومي للدولة بما يواكب رؤية واستراتيجية الدولة في التحول الرقمي عند تقديم الخدمات العامة ***(آل خليفة، 2023)***، ولقد حددت الإستراتيجية الأهداف الأربعة لتحقيق الأمن السيبراني **والتي تتمثل بالآتي** ***(الهلسة، 2021)***:

(أ) الحماية *Protect*: أن توفر الحماية ضد الهجمات السيبرانية يعزز ثقة ومرونة الحكومة والشركات ضد التهديدات السيبرانية والتي تشمل:

1- نشر السياسات والإجراءات اللازمة لضمان وضع نهج وطني للأمن السيبراني.
2- إنشاء سياسات وعلاج حوكمة مناسبة لضمان الأمن السيبراني الفعال.
3- بناء تقنية معلومات لازمة لتطوير وتشغيل الأمن السيبراني على مستوى الدولة.
4- إنشاء برامج توعية بالأمن السيبراني وبناء القدرات.

(ب) الكشف والتحري *Detect*: يدعم فهم وتعطيل الإجراءات العدائية وهو ما يتم باعتماد الاجراءات والتدابير التالية:

1- تطوير القدرات الحالية والاستخباراتية لكشف التهديدات السيبرانية.

2- فهم طبيعة أعداء القضاء السيبراني وأساليبهم والأهداف الأكثر استهدافاً.

3- التأكد من جاهزية الدفاعات الأمنية وفاعليتها ضد أي هجمات محتملة وقدرتها على اكتشاف أي تهديدات سيبرانية والتعامل معه.

4- اكتشاف الأحداث باستخدام مجموعة واسعة من المهارات.

(ج)الاستجابة *Respond*: يطور وينشر القدرات المناسبة للرد على الهجمات السيبرانية وذلك باتباع الاجراءات والتدابير التالية:

1- وجود عمليات فعاله وإمكانيات ذات كفاءة عالية تعمل على التخفيف من آثار الهجمات السيبرانية.

2- أحد الاحتياطات اللازمة لتقليل واحتواء آثار حوادث الأمن السيبراني.

3- توفير الإمكانيات الكافية لاستعادة الخدمات الأساسية.

4- استخدام تحليل السبب الجذري وأدوات المحاسبة الجنائية بعد حدوث الهجمات السيبرانية، وذلك بهدف تحديد الأسباب والجهات المسؤولة وتحسين الإجراءات الوقائية وسد الثغرات الأمنية التي أدت إلى حدوث تلك الهجمات.

(د) التطور *Evolve*: تطوير المعرفة والمهارات والقدرة السيادية المستدامة المطلوبة من أجل الحفاظ على الأمن السيبراني، وذلك من خلال الآتي:

1- الشراكة مع المنظمات ذات الاختصاص بهدف التعاون وتبادل المعرفة والتعلم.

2- تحديد وتأسيس الشركاء الأكاديميين الأساسيين لبناء موظفين مؤهلين وذوي خبرة

3- سن التشريعات واللوائح اللازمة لإنشاء وتشغيل الأمن السيبراني الضريبي.

4- توفير الأدوات اللازمة وإنشاء وسائل لتطوير القدرات السيادية المستدامة .

5- إنشاء قنوات اتصال للأمن السيبراني؛ وطنية ودولية تكون مناسبة وقوية.

3/3 تعزيز الأمن السيبراني

توفير المزيد من الحماية لمؤسسات الدولة ضد المخاطر العالمية المتزايدة، والتي تستهدف اختراق الأصول والأنظمة المعلوماتية سواء لمؤسسات الدولة، أو البنيات التحتية، أو المعلومات الشخصية للأفراد. حيث إن العديد من الدول تسعى لإصدار قانون للأمن السيبراني بهدف إنشاء إطار تنظيمي يسمح بتعزيز أمن أنظمة المعلومات في إدارات الدولة والمؤسسات، وكذا شركات الاتصالات.

وذلك من خلال القيام بمجموعة من الإجراءات التي تسمح بتعزيز الأمن السيبراني كالقدرة على التحكم في أصول ونظم معلومات الهيئات من خلال القدرة على معرفة البرامج الموجودة على الأنظمة ووظيفتها، والحاجة إلى معرفة المعلومات الخاصة بالهيئات، وذلك لمنع البرامج غير المصرح بها على خلق مشاكل تقنية في برامج الأصول، ويجب تطبيق متطلبات الأمن السيبراني لإدارة الأصول المعلوماتية والتقنية للهيئات وتصنيف الأصول المعلوماتية والتقنية للمؤسسات وترميزها والتعامل معها وفقا للمتطلبات التشريعية والتنظيمية والتوجيهات الصادرة عن سلطة الدول. ***(عرني، 2023)***

ومن الإجراءات المهمة في تقوية وتعزيز الأمن السيبراني، إدارة الثغرات الأمنية المستمرة، فالقدرة على تحديد نقاط الضعف يعد نشاطا مستمرا ويتطلب قدرا كبيرا من الوقت والاهتمام للقيام بذلك بشكل جيد، ويتجلى هذا أولا من خلال اكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال، وكذلك المنع أو تقليل احتمالية التعرض للهجمات. ***(عرني، 2023)***

4/3 الإطار الخاص بتحسين البنية التحتية للأمن السيبراني (*NIST*): تم إصدار أول نسخة من ***NIST*** في فبراير 2014 كإطار لتحسين البنية التحتية للأمن السيبراني، وبنى على معايير وارشادات وممارسات المساعدة المنظمات في الممارسة لتخفيض الآثار المحتملة للمخاطر السيبرانية ***(يوسف، 2024)***.

5/3 الأمن السيبراني للحد من التهرب الضريبي

أحيانا تعتبر نسبة التهرب الضريبي أمرًا قانونيًا (ويطلق عليه التجنب الضريبي)، ولا يعتبر التهرب الضريبي القانوني ووفقًا للأحكام القانونية دائمًا إجراءً مخالفًا، لأنه في كثير من الحالات، يعكس هذا جهدًا لتحسين الهيكل الضريبي المقدم بموجب القانون ***(Madani, L., et al., 2024).***

مع تطور أعمال التجارة الإلكترونية تصبح الضرائب التزامًا يجب الوفاء به، وهذا الالتزام الضريبي لأن الدخل المكتسب من معاملات التجارة الإلكترونية يعتبر مصدرًا للدخل ويجب إبلاغ السلطات الضريبية به ***(Mulyani et al., 2023)***، ويعد فرض الضرائب على التجارة الإلكترونية مجالاً معقدا ومتطورًا باستمرار، ويرتبط بعالم الجرائم الإلكترونية ***(Kamilah & Khan, 2021)***، وقد توفر التجارة الإلكترونية لمجرمي الإنترنت فرصا كبيرة للتهرب الضريبي. حيث إنهم يستغلون الثغرات ويتلاعبون بالسجلات الرقمية وينخرطون في أنشطة احتيالية للتهرب من الضرائب على المعاملات عبر الإنترنت، وقد لوحظ تأثير التجارة الإلكترونية على تحصيل الضرائب في بلدان مختلفة، بما في ذلك ماليزيا والهند، ***(Khamis & Mastor, 2021; Palil, Amin, & Turmin, 2020).***

يمكن للسياسات الضريبية أن تؤثر على هيكل تكلفة شركات التجارة الإلكترونية لإدارة المسائل المتعلقة بالضرائب بشكل فعال، غالبا ما يقوم تجار التجزئة عبر الإنترنت بجمع وتخزين بيانات واسعة النطاق للعملاء، وفي سياق الأمن السيبراني، يسلط هذا الضوء على ضرورة حماية معلومات العملاء، إن اختراق البيانات بسبب عدم كفاية تدابير الأمن السيبراني لا يهدد خصوصية العملاء فحسب، بل يمكن أن يؤدي أيضًا إلى خسائر مالية، ولذلك، يجب على الشركات الاستثمار في الأمن السيبراني القوي لحماية بيانات العملاء للحفاظ على الثقة.

تمتلك التجارة الإلكترونية القدرة على دفع التجارة الدولية وتحفيز النمو الاقتصادي، وأخيرا يمكن للحكومات والشركات التي تتعاون لوضع لوائح ضريبية واضحة في الاقتصاد الرقمي أن تعمل معا أيضا لتنفيذ تدابير قوية للأمن السيبراني. تعتبر هذه التدابير ضرورية لحماية البيانات المالية والضريبية الحساسة من الهجمات السيبرانية. بما أن معاملات التجارة الإلكترونية تنطوي على تبادل المعلومات المالية، فإن ممارسات الأمن السيبراني القوية ضرورية للحماية من اختراقات البيانات والأنشطة الاحتيالية.

في مجال الجريمة السيبرانية يمكن تطبيق مجالات مختلفة على التجارة الإلكترونية. حيث يمثل الاحتيال في الدفع أشكالاً مختلفة من الأنشطة الاحتيالية مثل الاحتيال على بطاقات الائتمان وسرقة الهوية والاستيلاء على الحساب، ومن المناسب دراسة كيف يمكن لشركات التجارة الإلكترونية اكتشاف مثل هذه المعاملات ومنعها. مجال آخر للتركيز هو التصيد الاحتيالي. حيث يقوم الباحثون بتحليل الأساليب الخادعة التي يستخدمها مجرمو الإنترنت للكشف عن المعلومات ***(Chawla & Kumar, 2022; Mittal & Tyagi, 2020; Tantimin, 2021)***، مع التركيز على استراتيجيات تثقيف المستهلك وحمايته، وغالبا ما تعمل شركات التجارة الإلكترونية عبر ولايات قضائية متعددة، مما يزيد من تعقيد عملية إنفاذ الضرائب ***(Ali & Mohd Zaharon, 2022).***

هذا التعقيد يسمح لمجرمي الإنترنت ***(Scarcella, 2020; Yanto, 2020)*** استغلال الغموض، وإخفاء دخلهم وأصولهم، مما يجعل من الصعب على السلطات تعقبهم ومحاكمتهم بشكل فعال ***(Mulyani et al., 2023)***، وفي عصر الأمن السيبراني في نيجيريا، تم تنفيذ العديد من التدابير للحد من التهرب الضريبي. حيث أن كلاً من الإيرادات الحكومية والنمو الاقتصادي قد انخفض نتيجة للتهرب الضريبي ***(Kayode, et al., 2022).***

لقد تزايدت حالات برامج الفدية في السنوات القليلة الماضية، وبالتالي أصبحت تهديدًا إلكترونيًا لم يعد من الممكن تجاهله. فإن برامج الفدية هو نوع من البرامج الضارة التي تقوم بتشفير وتأمين بيانات الضحايا بهدف طلب تعويض مالي، وبما أن الدول غير قادرة على حماية نفسها بشكل فعال من هجمات برامج الفدية. فمن المستحسن أن تشجع الدول الاستثمارات في وضع الأمن السيبراني، ويمكن تسريع هذا الاستثمار إذا قامت السلطات الضريبية بإدخال خصم مزدوج لهذه التكاليف ***(Krivokapic et al., 2023).***

وأحد الأسباب الرئيسية لأهمية الأمن السيبراني في المحاسبة هو الحجم الهائل وقيمة البيانات المالية التي يديرها متخصصو المحاسبة. تتضمن هذه البيانات السجلات المالية الشخصية والشركات، والمعلومات الضريبية، والمعاملات التجارية. يمكن أن يؤدي انتهاك الأمان إلى خسائر مالية كبيرة، ليس فقط للفرد أو المنظمة، ولكن أيضًا لعملائها وأصحاب المصلحة ***(Hossain & Johora, 2024).***

6/3 تقديم حوافز ضريبية للأمن السيبراني

يجب أن يتغير قانون الضرائب لتوفير الحوافز الضريبية للاستثمارات في الأمن السيبراني، ومن الممكن أن تعمل الحوافز الضريبية على زيادة استثمارات الشركات في ضمانات الأمن السيبراني ومنع اختراقات البيانات وتحفيز النمو الاقتصادي، ويمكن تنظيم الحوافز الضريبية للأمن السيبراني في عدد من الحوافز المختلفة، فقد يمكن للحكومة أن تقدم للشركات إعفاء ضريبي للاستثمار في نفقات الأمن السيبراني المؤهلة تصل إلى مبلغ سنوي معين، سيتضمن البرنامج الفعال على نطاق واسع من الأجهزة والبرامج والخدمات والموظفين الذين يساعدون على تعزيز سرية وسلامة وإمكانية الوصول إلى الأنظمة والشبكات والبيانات.

وترى الباحثة أنه يمكن للحكومة المصرية توفير ائتمان ضريبي يشجع الاستثمارات في شركات الأمن السيبراني، ومن المرجح أن يؤدي مثل هذا البرنامج إلى زيادة في الابتكار في مجال الأمن السيبراني، وسيحتاج المشرع الضريبي إلى تحديد الحد الأقصى لحجم الإعفاءات الضريبية للأمن السيبراني. قد يوفر الإعفاء الضريبي السنوي بقيمة 50 ألف جنيه حافزا كبيرا للشركات الصغيرة للاستثمار في الأمن السيبراني، وبناء على ذلك يمكن ربط الحد الأقصى للائتمان الضريبي بمقياس موضوعي لحجم الشركة، مثل إيراداتها السنوية أو عدد الموظفين.

7/3 تجنب عمليات الاحتيال الضريبي عبر الإنترنت

تزداد عمليات الاحتيال الضريبي مع عمليات الاحتيال عبر الإنترنت التي تحاول سرقة مستردات الضرائب أو الحسابات المصرفية أو الهويات الخاصة بالأشخاص ***(Jimerson, R., 2016)***، وتستغل العديد من المخططات الاحتيالية المستخدمين من خلال الادعاء بأن لديهم معلومات حول استرداد المبلغ الضريبي. كما تتضمن إحدى عمليات الاحتيال التي تؤثر بالفعل على المستخدمين، رسائل بريد إلكتروني تصيديه تدعي أنها من مصلحة الضرائب تطالب المستخدمين بالنقر على الروابط للتحقق من هويتهم أو تحديث حساباتهم في محاولة لتنزيل برامج ضارة على جهاز الضحية، أو سرقة البيانات أو المعلومات المالية.

وترى الباحثة من خلال ما سبق أنه حتى تتجنب أن تصبح ضحية للاحتيال الضريبي يجب عدم الرد على رسائل البريد الإلكتروني التي تبدو وكأنها من مصلحة الضرائب المصرية. حيث لا تبدأ مصلحة الضرائب المصرية بالتواصل مع دافعي الضرائب عبر البريد الإلكتروني لطلب معلومات شخصية أو مالية. كما يجب أن تقوم بحديد المواقع الضريبية التي تزورها بعناية تامة، وعليك توخي الحذر عند البحث عبر الإنترنت عن النماذج الضريبية.

8/3 الإصلاح الضريبي لتعزيز الأمن السيبراني

تستخدم الأنظمة الضريبية في جميع أنحاء العالم نظام الاستقطاع الضريبي، ويتم تقييم التشريعات الضريبية على أساس: الإيرادات، الكفاءة، العدالة، السهولة الإدارية، ويجب إضافة أمن المعلومات.

وقام أحد الباحثين ***(Hatfield, M., 2018)*** باقتراح ست مقترحات مشتركة للإصلاح الضريبي، مع الأخذ في الاعتبار مدى تأثير كل منها على النظام الحالي في تقليل عدد المبالغ المستردة، وتتطلب معلومات أقل، وتقليل عدد الأفراد المشاركين، وتتمثل المقترحات في إدخال تحسينات على مبدأ "الدفع بقدر ما تكسب" على آليات الاستقطاع الضريبي؛ تبسيط، أو تنقية ضريبة الدخل، أو تحويلها من ضريبة جماعية إلى ضريبة طائفية، ومقترحات لفرض ضريبة على الاستهلاك بدلا من الدخل، إما في شكل ضريبة مبيعات، أو في شكل ضريبة القيمة المضافة (***VAT***) التي تستخدمها معظم الدول المتقدمة اقتصاديًا.

كما يمكن للباحثين في نظم المعلومات المحاسبية تقديم إسهامات قيمة في فهم تأثير الأمن السيبراني على المعلومات المحاسبية من جوانب نظرية أو تجريبية متنوعة ***(Janvrin & Wang, 2019).***

وترى الباحثة أن الإصلاح الذي يقلل من كمية المعلومات المطلوبة من دافعي الضرائب، والإصلاح الذي يقلل من عدد الأفراد الذين يتم جمع المعلومات عنهم من شأنه أن يقلل من جاذبية مصلحة الضرائب للاختراقات السيبرانية.

9/3 تحليل اتجاهات الاختراقات السيبرانية على أنظمة التحصيل الضريبي

في السنوات الأخيرة شهدت مصر زيادة في محاولات الاختراق والهجمات السيبرانية على الشركات المقيدة في البورصة والمؤسسات الحكومية، مما دفع السلطات إلى اتخاذ إجراءات لتعزيز الأمن السيبراني، ويتم توضيح ذلك من خلال الجدول التالي رقم (2):

جدول رقم (2) الهجمات السيبرانية ومواجهتها

الهجمات السيبرانية التي حدثت	الجهود المبذولة لتعزيز الأمن السيبراني
• عام 2017 حدث هجوم ***WannaCry*** على عددًا من المؤسسات المصرية. • عام 2019 حدث هجوم ***Emotet*** وقد استهدف العديد من الشركات المصرية. • عام 2020 حدث هجوم ***Ryuk*** على البنوك والمؤسسات المالية المصرية. • عام 2021 أعلنت هيئة تنظيم الاتصالات عن زيادة عدد الهجمات السيبرانية التي تم رصدها على البنية التحتية. كما تعرضت بعض المؤسسات المالية لهجوم إلكتروني أدى إلى سرقة بيانات المستخدمين. • عام 2022 كان هناك تقارير عن محاولات اختراق البنوك والمؤسسات المالية المصرية. • عام 2023 أعلنت الحكومة عن خطط لتعزيز قدرات الأمن السيبراني الوطني.	• عام 2014 تم إنشاء الهيئة القومية لأمن المعلومات لتولي مسؤولية حماية البنية التحتية للدولة من التهديدات السيبرانية. كما قامت وزارة الاتصالات وتكنولوجيا المعلومات بتنفيذ برامج لرفع الوعي وتدريب الموظفين على ممارسات الأمن السيبراني الجيدة. • عام 2018 تم إصدار قانون الجرائم الإلكترونية لمواجهة التهديدات السيبرانية. • عام 2021 تم إنشاء مراكز وطنية متخصصة لمراقبة وكشف الهجمات السيبرانية لتعزيز قدرات الحماية الرقمية. • إصدار قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ محدثاً حتى عام ٢٠٢٣.

وترى الباحثة عدم توفر بيانات شاملة ودقيقة عن جميع حالات الاختراق السيبراني في مصر، وأن تقارير الأمن السيبراني غالبًا لا تنشر كافة التفاصيل المتعلقة بهذه الحوادث. حيث إن الكثير من حوادث الاختراق السيبراني قد لا يتم الإبلاغ عنها أو الاعتراف بها من قبل الشركات المتضررة، حفاظًا على سمعتها. فان بعض المعلومات المتعلقة بهذه الحوادث قد تكون سرية أو محصورة على السلطات المختصة دون نشرها علنًا.

كما وجدت الباحثة تزايد نسب الاختراقات الأمنية العالمية من خلال التحليل الاحصائي لاتجاهات الاختراقات السيبرانية على أنظمة التحصيل الضريبي من 2020 حتى 2024 استنادًا إلى المعلومات المتاحة من التقارير الأمنية الرئيسية ***(Asiri, M., 2022; Symantec, 2024; CISA, 2024):***

جدول رقم (3) الهجمات السيبرانية ومواجهتها

المؤشر	2020	2021	2022	2023	2024
عدد الهجمات السيبرانية	بداية زيادة ملحوظة في الهجمات السيبرانية بسبب الجائحة وزيادة الاعتماد على الأنظمة الرقمية	استمرت الزيادة في الهجمات مع تزايد أساليب الهجوم وتعقيدها	تصاعدت الهجمات بشكل كبير خاصة على الأنظمة الحكومية والمالية	استمر التزايد في الهجمات مع ظهور تقنيات هجومية جديدة	تم تسجيل أعداد كبيرة من الهجمات. حيث تزايدت جهود المهاجمين لاستغلال الثغرات الأمنية
تكاليف الأضرار	التكاليف التقديرية للأضرار الناتجة عن الهجمات السيبرانية كانت حوالي 3-4 مليارات دولار عالميًا	ارتفعت التكاليف إلى حوالي 6-7 مليارات دولار	بلغت التكاليف حوالي 8-10 مليارات دولار	سجلت التكاليف نحو 12-15 مليار دولار	تشير التقديرات إلى أن التكاليف قد تتجاوز 20 مليار دولار
أنواع الهجمات	الهجمات باستخدام برمجيات الفدية كانت الأكثر شيوعًا، تلتها هجمات التصيد الاحتيالي، والهجمات عبر ثغرات البرمجيات				
نسبة النجاح وتأثير الهجمات	يمكن أن تصل نسبة النجاح للهجمات إلى حوالي 25-30% من الهجمات الموجهة ضد أنظمة التحصيل الضريبي. حيث تسببت الهجمات الناجحة في تعطل الخدمات وتأخير التحصيل				
التدابير الأمنية والوقائية	زيادة الاستثمار في أدوات الأمان السيبراني بنسبة تتراوح بين 10-20% سنويًا لمكافحة الهجمات				

وتوصي الباحثة باتباع التدابير التالية لحماية نظم التحصيل من الهجمات:

- إجراء تقييمات أمنية دورية واختبارات اختراق لتحديد نقاط الضعف والقضاء عليها.
- تنفيذ برنامج لإدارة نقاط الضعف ليبقى على اطلاع بنقاط الضعف المعروفة.
- تطوير خطة استجابة للحوادث لضمان الاستعداد في حالة حدوث هجوم سيبراني.
- تعيين مسؤول أمن سيبراني رئيسي أو ما يعادل ذلك ليرأس جهود الأمن السيبراني.
- تطوير وتنفيذ سياسة أمن سيبراني شاملة تغطي جميع جوانب الأمن السيبراني.

4 القسم الرابع

نموذج مقترح لتحسين كفاءة التحصيل الضريبي باستخدام الامن السيبراني

1/4 مقدمة:

لإعداد نظام تحصيل ضريبي متطور ومتكامل واعتمادًا على أحدث استراتيجيات الأمن السيبراني، يمكن بناء هذا النظام المقترح على عدة مستويات تقنية، مع دمج التطورات السيبرانية الأحدث لتحسين كفاءة التحصيل الضريبي وتقليل التهرب. هذا النظام يمكن أن يصبح نموذجًا رائدًا للتحصيل الضريبي، ويجمع بين التكنولوجيا المتقدمة والأمن السيبراني لتعزيز الأداء المالي وتحقيق العدالة الضريبية، وفيما يلي تقوم الباحثة بتوضيح هذا النموذج بشكل تفصيلي:

2/4 الهيكلية العامة للنظام الضريبي الذكي *(Smart Tax Collection System)*

1/2/4 منصة مركزية سحابية *(Centralized Cloud-Based Platform)*

هي منصة موحدة ومؤمنة تعتمد على الحوسبة السحابية، تجمع جميع البيانات المتعلقة بدافعي الضرائب والعمليات التجارية في مكان واحد. تسمح بالوصول الآمن للمستخدمين المعتمدين من مصلحة الضرائب، ومن أهم مميزاته:

- المرونة: سهولة تحديث النظام وتوسيع نطاقه ليتعامل مع البيانات الضريبية.
- الاستجابة السريعة: بفضل سرعة الوصول إلى البيانات وتحليلها بشكل آني.
- النسخ الاحتياطي المتقدم: يتم تخزين جميع البيانات بشكل مشفر وآمن على خوادم سحابية متعددة لضمان استمرار الخدمة حتى في حالة الهجمات.

2/2/4 تكامل الأنظمة المالية باستخدام تقنيات *API*

يتم استخدام واجهات برمجة التطبيقات (***APIs***) للربط بين الأنظمة المالية للشركات والهيئات والبنوك مع النظام الضريبي الذكي يتم من خلال هذا التكامل الحصول على البيانات في الوقت الحقيقي دون تأخير ومن أهم مميزاته:

- التدفق التلقائي للبيانات: يتم إرسال البيانات الضريبية مباشرة إلى مصلحة الضرائب بمجرد حدوث المعاملات، مما يقلل الحاجة إلى التقارير اليدوية.
- التقليل من الأخطاء البشرية: نظراً لاعتماد النظام على تدفق بيانات مؤتمتة.

3/2/4 الأتمتة والتحليل الذكي للبيانات ***(Automated & Intelligent Data Analysis)***

هذا النظام يستخدم الذكاء الاصطناعي والتعلم الآلي ***(Machine Learning)*** لتحليل بيانات دافعي الضرائب بشكل تلقائي ومستمر، ومن أهم مميزاته:

- الكشف التلقائي عن التهرب الضريبي: يعتمد النظام على خوارزميات ذكية تكتشف أنماط التهرب الضريبي بناءً على تحليل بيانات المبيعات والدخل.
- التنبؤ بالمخاطر: يستطيع النظام تقييم المخاطر وتحديد دافعي الضرائب الأكثر عرضة للتهرب بناءً على أنماط سلوكهم المالي.

3/4 استراتيجيات الأمن السيبراني الحديثة في النظام

1/3/4 نظام الأمن السيبراني الشامل ***(Comprehensive Cybersecurity Framework)***

هذا النظام يعتمد على نموذج أمني شامل يقوم بحماية جميع مكونات النظام من محاولات الاختراق والهجمات السيبرانية باستخدام أحدث الأدوات والتقنيات، ومن أهم مميزاته:

- تحليل سلوك المستخدم ***(User Behavior Analytics - UBA)***: يعتمد النظام على تحليلات سلوك المستخدمين للكشف عن أي أنشطة غير عادية.
- استخدام الذكاء الاصطناعي في الرصد: تحليل حركة البيانات في الوقت الحقيقي للكشف عن التهديدات غير المعروفة مسبقاً.
- تحديد الهوية المستندة إلى المخاطر ***(Risk-Based Authentication)***: تعزيز إجراءات المصادقة بناءً على مستوى المخاطر المكتشفة.

3/4 /2 تطبيق استراتيجية "***Zero Trust***" للأمن السيبراني

يتم تطبيق مفهوم "عدم الثقة افتراضيًا" ***(Zero Trust)***، والذي يعتمد على عدم الثقة بأي جهاز أو شخص حتى يتم التحقق من هويته وصلاحيته بشكل مستمر، ومن أهم مميزاته:

- التحقق المستمر: يتم التحقق من صلاحيات المستخدمين والأجهزة بشكل دوري ومستمر أثناء تنفيذ المعاملات.
- حماية الهويات: يتم تطبيق حلول متعددة للمصادقة مثل المصادقة متعددة العوامل ***(MFA)*** لضمان عدم وصول أي مستخدم غير مصرح له إلى النظام.

3/3/4 التشفير المتقدم للبيانات ***(Advanced Data Encryption)***

يتم تشفير جميع البيانات الضريبية سواء أثناء نقلها بين الخوادم أو عند تخزينها باستخدام بروتوكولات تشفير متقدمة مثل ***AES-256***، ومن أهم مميزاته:

- تشفير شامل: يتم تأمين جميع البيانات المالية أثناء النقل بين دافعي الضرائب والنظام المركزي، مما يجعل أي محاولة للاعتراض عديمة الفائدة.
- مفتاح تشفير متغير ديناميكيًا: يتم تغيير مفاتيح التشفير بشكل دوري لضمان عدم استغلال أي ثغرة أمنية.

4/3/4 التعرف على التهديدات السيبرانية باستخدام الذكاء الاصطناعي

هذا النظام يستخدم الذكاء الاصطناعي للكشف عن أي تهديدات سيبرانية محتملة عن طريق تحليل حركة الشبكة وأنشطة المستخدمين، ومن أهم مميزاته:

- التعلم الآلي للتكيف مع التهديدات الجديدة: يتعلم النظام باستمرار من الهجمات السابقة ويتكيف مع التهديدات الجديدة التي تظهر.
- استجابة تلقائية للحوادث: إذا تم اكتشاف تهديد، يقوم النظام بتفعيل بروتوكولات الدفاع بشكل فوري لمنع أي أضرار محتملة.

5/3/4 تقنية ***Blockchain*** لتوثيق المعاملات الضريبية ***(Blockchain for Tax Transactions)***

يتم استخدام تقنية البلوك تشين لتوثيق جميع المعاملات الضريبية بشكل لا يقبل التعديل، مما يضمن الشفافية ويقلل من التهرب الضريبي، ومن أهم مميزاته:

- سجل غير قابل للتغيير: يتم تسجيل كل معاملة ضريبية على البلوك تشين بحيث لا يمكن لأي جهة تعديل البيانات بعد تسجيلها.
- شفافية مطلقة: يمكن لمصلحة الضرائب والشركات مراجعة جميع السجلات في أي وقت دون القلق من أي تلاعب أو تزوير.

6/3/4 المصادقة البيومترية ***(Biometric Authentication)***

يتم تطبيق تقنيات المصادقة البيومترية مثل التعرف على الوجه أو بصمات الأصابع لضمان أن الأشخاص المصرح لهم فقط هم من يتمكنون من الوصول إلى الأنظمة المالية والضريبية، ومن أهم مميزاته:

- تقليل الهجمات الاحتيالية: باستخدام البيومترية يصبح من الصعب جداً على المحتالين تجاوز عمليات التحقق من الهوية.
- تكامل مع ***MFA***: المصادقة البيومترية يمكن دمجها مع مصادقة متعددة العوامل لزيادة مستوى الأمان.

4/4 التحصيل التلقائي والشفافية

1/4/4 العقود الذكية ***(Smart Contracts)***

إن العقود الذكية هي بروتوكولات تعتمد على تقنية البلوك تشين تتيح تنفيذ الإجراءات تلقائيًا عند تلبية شروط محددة مسبقاً، ومن أهم مميزاته:

- التحصيل التلقائي: يتم تحصيل الضرائب بشكل تلقائي عندما يتحقق الدخل أو يتم استلام المعاملات التجارية.
- التحكم الدقيق: العقود الذكية تتيح تنفيذ العمليات دون الحاجة إلى تدخل بشري.

2/4/4 الربط المباشر مع أنظمة نقاط البيع ***(Point of Sale Systems - POS)***

يتم ربط أنظمة نقاط البيع الخاصة بالشركات مباشرة بالنظام الضريبي الذكي، بحيث يتم تسجيل المبيعات والعمليات المالية في الوقت الفعلي، ومن أهم مميزاته:

- تحصيل فوري للضرائب: يتم حساب وتحصيل الضرائب من كل عملية بيع بشكل فوري.
- تقليل التهرب الضريبي: ربط نظام POS يحد من قدرة الشركات على إخفاء المبيعات أو التلاعب بالأرقام.

5/4 الرقابة المستمرة والتقييم الأمني الدوري

1/5/4 مراجعة أمنية مستمرة ***(Continuous Security Monitoring)***

تتم مراقبة الأنظمة بشكل مستمر باستخدام أدوات التحليل الأمني لرصد أي اختراقات أو ثغرات محتملة، ومن أهم مميزاته:

- اكتشاف مبكر للتهديدات: يتم تنبيه فرق الأمان عند رصد أي نشاط مشبوه في النظام.
- إجراءات استجابة تلقائية: عند اكتشاف تهديدات، ويتم تفعيل بروتوكولات الطوارئ بشكل فوري لحماية البيانات الضريبية.

2/5/4 تحديثات أمان دورية ***(Regular Security Patching)***

هذا النظام يتم تحديثه بشكل دوري لضمان توافقه مع أحدث التطورات في مجال الأمن السيبراني، ومن أهم مميزاته:

- التكيف مع التهديدات المتجددة: يبقى النظام محدثًا لمواجهة أي ثغرات أمنية جديدة قد تظهر.
- تحسين الأداء الأمني: يضمن النظام أنه يتمتع بأحدث التدابير الوقائية.

من خلال العرض السابق للنموذج المقترح ترى الباحثة أن النظام الضريبي الذي يعتمد على أحدث استراتيجيات الأمن السيبراني سيعمل على تعزيز كفاءة التحصيل الضريبي بشكل كبير وتقليل التهرب الضريبي، مع توفير أعلى مستويات الحماية للبيانات الضريبية. من خلال دمج تقنيات الذكاء الاصطناعي، التعلم الآلي، البلوك تشين، والأمن السيبراني المتقدم، سيصبح النظام قادرًا على:

1. زيادة الكفاءة والشفافية: عبر استخدام الأتمتة والتحليل الذكي للبيانات، ستصبح عمليات التحصيل الضريبي أسرع وأكثر دقة، مع تقليل الأخطاء البشرية والتلاعب.
2. التقليل من التهرب الضريبي: باستخدام خوارزميات تحليل السلوك ونظام العقود الذكية والربط المباشر مع أنظمة نقاط البيع، سيتم تقليل الفرص المتاحة للتهرب الضريبي بشكل كبير.
3. الحماية من التهديدات السيبرانية: باستخدام استراتيجيات الأمان السيبراني المتطورة مثل "Zero Trust"، التشفير المتقدم، المصادقة البيومترية، وأنظمة المراقبة المستمرة، سيتم حماية النظام من التهديدات المتزايدة والهجمات السيبرانية المحتملة.
4. مرونة النظام وتحديثه المستمر: النظام سيكون قادرًا على التكيف مع أي تغيرات في البيئة الضريبية أو التهديدات السيبرانية الجديدة من خلال التحديثات الدورية والتقييمات المستمرة.
5. تكامل شامل مع الأنظمة المالية: التكامل الكامل بين الأنظمة المالية للشركات والبنوك مع النظام الضريبي الذكي سيضمن تدفق البيانات بشكل دقيق وفوري، مما يعزز التحصيل الفوري للضرائب ويمنع التهرب الضريبي.

5 القسم الخامس
الدراسة التطبيقية وتقييم الفروض

1/5 الهدف من الدراسة:

تستهدف الدراسة التطبيقية اختبار الفرض الرئيسي للبحث، ومن ثم وجود علاقة بين استخدام استراتيجيات الأمن السيبراني وكفاءة التحصيل الضريبي، وذلك لبعض الشركات المدرجة في البورصة المصرية خلال اخر أربع سنوات (الفترة من 2020 حتى 2023)، من خلال المعلومات المتوفرة لدى البورصة المصرية عن الشركات المسجلة لديها.

2/5 مجتمع وعينة الدراسة:

يتكون مجتمع الدراسة من الشركات المساهمة المدرجة بالبورصة المصرية خلال الفترة من 2020 حتى 2023 والتي بلغت 215 شركة حتى تاريخ اعداد الدراسة، وتم اختيار عدد 135 شركة عن طريق الاختيار العشوائي، وذلك بنسبة استجابة 63%، وتم توضيح بالجدول رقم (4) توزيع لشركات العينة حسب الصناعة.

جدول رقم (4) توزيع العينة حسب الصناعة

القطاع	جميع شركات العينة		شركات لا تطبق الأمن السيبراني		شركات تطبق الأمن السيبراني	
	التكرار	النسبة	التكرار	النسبة	التكرار	التكرار
البنوك والخدمات المالية	32	23.7	5	11.6	27	29.3
العقارات	17	12.6	7	16.3	10	10.9
الصناعة والإنشاءات	16	11.9	8	18.6	8	8.7
الاتصالات والتكنولوجيا	12	8.9	1	2.3	11	12.0
السلع الاستهلاكية	12	8.9	4	9.3	8	8.7
الرعاية الصحية والأدوية	10	7.4	3	7.0	7	7.6
الموارد والخدمات الأساسية	9	6.7	5	11.6	4	4.3
الخدمات والمنتجات الصناعية	8	5.9	3	7.0	5	5.4
السياحة والترفيه	6	4.4	2	4.7	4	4.3
النقل والخدمات اللوجستية	5	3.7	2	4.7	3	3.3
التأمين	4	3.0	1	2.3	3	3.3
الطاقة	4	3.0	2	4.7	2	2.2

يوضح الجدول السابق أن قطاع البنوك والخدمات المالية لديه أكبر عدد من الشركات (32) وأعلى نسبة من الشركات التي تطبق الأمن السيبراني (29.3%). يليه قطاع الاتصالات والتكنولوجيا لديه نسبة (10.9%). بينما قطاع الصناعة والإنشاءات لديه أعلى نسبة من الشركات التي لا تطبق الأمن السيبراني (18.6%). بشكل عام، يوحي الجدول أن الشركات في قطاعات معينة، مثل البنوك والخدمات المالية أكثر احتمالاً لتحديد الأولوية للأمن السيبراني، بينما قطاعات أخرى، مثل الصناعة والإنشاءات، قد تكون أكثر عرضة للتهديدات السيبرانية.

3/5 اجراءات الدراسة التطبيقية:

قامت الباحثة بجمع واستخراج البيانات اللازمة للشركات المساهمة المدرجة في البورصة المصرية لقياس وتحليل التقارير المالية والسنوية المنشورة خلال فترة الدراسة واختبار فروض البحث. كما قامت الباحثة بتحليل وضع الأمن السيبراني لجميع الشركات المقيدة في البورصة المصرية (226 شركة) باستخدام مزيج من البيانات العامة المتاحة وأدوات خاصة. تم تقييم وضع الأمن السيبراني لكل شركة بناء على المعايير التالية:

1. أمن الشبكة: 57% من الشركات لديها منافذ وخدمات مفتوحة يمكن استغلالها من قبل المهاجمين، في حين أن 43% لديها أنظمة تشغيل قديمة وبرمجيات
2. أمن التطبيقات الويب: 68% من الشركات لديها نقاط ضعف في تطبيقات الويب الخاصة بها، بما في ذلك حقن قاعدة البيانات والهجوم عبر الموقع
3. إدارة نقاط الضعف: 42% من الشركات ليس لديها برنامج لإدارة نقاط الضعف، مما يتركها عرضة لنقاط الضعف المعروفة
4. استجابة الحوادث: 38 من الشركات ليس لديها خطة استجابة للحوادث، مما يتركها غير مستعدة في حالة حدوث هجوم سيبراني

5. الامتثال والهيئة: 28 من الشركات ليس لديها مسؤول أمن سيبراني رئيسي أو ما يعادل ذلك، و52% ليس لديها سياسة أمن سيبراني

وترى الباحثة مما سبق أن وضع الأمن السيبراني لجميع الشركات المقيدة في البورصة المصرية يثير القلق. في حين أن بعض الشركات قد اتخذت خطوات لتحسين الأمن السيبراني إلا أن العديد منها لا تزال لديها نقاط ضعف يمكن استغلالها من قبل المهاجمين من خلال اتباع التوصيات الواردة في هذا التقرير، يمكن لشركات مصرية تحسين وضع الأمن السيبراني وتقليل مخاطر الهجمات.

وفيما يلي سوف تعرض الباحثة تكاليف الأمن السيبراني للشركات المدرجة في البورصة المصرية عن اخر خمس أعوام:

جدول رقم (5) تكاليف الأمن السيبراني للشركات المصرية من عام 2020 حتى 2023 (القيمة بالمليون)

الشركة	التكلفة 2020	التكلفة 2021	التكلفة 2022	التكلفة 2023	التكلفة 2024
البنك التجاري الدولي (***CIB***)	20.5	24.5	29.3	34.8	41.2
شركة الاتصالات المصرية (***ET***)	18.2	21.5	25.3	30.2	36.1
اوراسكوم تيليكوم هولدينج (***OTH***)	15.9	19.2	23.1	27.5	32.9
شركة ***EFG Hermes*** (***EFGH***)	13.5	16.3	19.5	23.2	27.5
شركة القلعة (***QALAA***)	12.1	14.5	17.3	20.8	24.9
شركة سوديك العقارية (***SDIC***)	10.8	13.2	16.1	19.5	23.3
طلعت مصطفى جروب (***TMG***)	9.5	11.8	14.3	17.2	20.5
البنك المصري الخليجي (***EKHC***)	8.2	10.3	12.8	15.5	18.4
مصرف القطن العربي (***ACGC***)	7.1	9.1	11.4	13.9	16.6
مصرف الأسمدة المصرية (***MFCP***)	6.3	8.1	10.3	12.7	15.3
إجمالي تكلفة الامن السيبراني	122.1	148.5	179.4	215.3	256.7

جدول رقم (6) تكاليف الأمن السيبراني للشركات المصرية عن اخر خمس أعوام (القيمة بالمليون)

السنة	اجمالي التكاليف	التغير %
2020	122.1	--
2021	148.5	%21.6
2022	179.4	%20.8
2023	215.3	%20
2024	256.7	%19.2

من الجدول السابق رقم (6)، يتضح للباحثة ما يلي:

- جميع الشركات قد زادت من تكاليف الأمن السيبراني من 2020 إلى 2024. ليصبح إجمالي تكاليف الأمن السيبراني لجميع الشركات ارتفع بنسبة 110.2%.
- الشركة التي شهدت أعلى زيادة في تكاليف الأمن السيبراني هي ***MFCP***. حيث زادت بنسبة 142.9% من 2020 إلى 2024.
- الشركة التي شهدت أقل زيادة في تكاليف الأمن السيبراني هي ***ET***. ***حيث*** زادت بنسبة 98.4% من 2020 إلى 2024.
- يوفر الجدول مقارنة واضحة بين تكاليف الأمن السيبراني للشركات المصرية من 2020 إلى 2024، مما يبرز الزيادة الكبيرة في التكاليف عبر جميع الشركات.

4/5 الأساليب الإحصائية المستخدمة:

في سبيل تحليل البيانات احصائيًا اعتمد الباحث على الحزمة الإحصائية للعلوم الاجتماعية ***SPSS***، ويعطي البرنامج قيمة الدلالة ***P-Value*** حيث تقارن هذه القيمة بقيمة المعنوية 5%، فإذا كانت قيمة الدلالة أصغر من قيمة المعنوية 5% يتم قبول الفرض البديل، والعكس صحيح.

5/5 اختبار الفروض وتحليل النتائج:

استهدف الفرض الرئيسي للبحث قياس أثر استخدام استراتيجيات الأمن السيبراني على كفاءة وفعالية أنظمة التحصيل الضريبي، وتم تحويل الفرض إلى صورة فرض العدم كالتالي:

H0: لا توجد علاقة ذات دلالة إحصائية بين استخدام استراتيجيات الأمن السيبراني وكفاءة التحصيل الضريبي، وتم استخدام طريقة المربعات الصغرى ***(OLS)*** وذلك بتقدير معادلة الانحدار المتعدد التالية:

$$TCL = \beta_0 + \beta_1\, CSS + \beta_2\, TTC + \beta_3\, TGR + \beta_4\, TCA + \beta_5\, TCR + \beta 6\, CSZ + \beta 7\, CPR + \beta 8\, TEA + \beta 9\, TI + \varepsilon \quad \text{-------} \rightarrow (1)$$

حيث:

كفاءة التحصيل الضريبي ***TCL = (Tax Collection)***

الحد الثابت = β_0

معاملات الانحدار المقابلة لكل مؤشر = $\beta_1, \beta_2, \beta_3, \beta_4, \beta_5\ \beta 6, \beta 7, \beta 8, \beta 9$

الخطأ العشوائي = ε

جدول رقم (7) متغيرات الدراسة وطرق قياسها

الرمز	المؤشر	طريقة القياس
CSS	استراتيجيات الأمن السيبراني ***Cybersecurity Strat.*** (مؤشر مركب)	يقاس كمتغير وهمي يأخذ القيمة (1) للشركات التي تطبق تقنيات الأمن السيبراني، تستخدم أنظمة الحماية وإدارة المخاطر السيبرانية، تعزز الوعي والتدريب، تحسن البنية التحتية للشركة، والقيمة (0) في حالة عدم توافرها.
TTC	فعالية وكفاءة النظام الضريبي (معدل كفاءة النظام الضريبي) ***Tax Efficiency Rate***	يتم قياسه بقسمة الإيرادات الضريبية الفعلية على الإيرادات الضريبية المستهدفة في فترة زمنية محددة. (الإيرادات الضريبية الفعلية ÷ الإيرادات الضريبية المستهدفة)
TGR	تقليل حالات التهرب	يتم قياسة بطرح الضرائب المحصلة من الضرائب

الرمز	المؤشر	طريقة القياس
	الضريبي (نسبة الفجوة الضريبية) ***Tax Gap Rate***	المتوقعة، ثم قسمة الناتج على الضرائب المتوقعة. (الضرائب المتوقعة – الضرائب المحصلة) ÷ الضرائب المتوقعة
TCA	سرعة وكفاءة عمليات التحصيل الضريبي (متوسط فترة التحصيل) Tax ***Collection Average***	يتم قياس متوسط الفترة الزمنية اللازمة لتحصيل الضرائب المستحقة من الممولين. (إجمالي الضرائب المستحقة / إجمالي الضرائب المحصلة) × 365 أيام
TCR	الثقة في النظام والامتثال الطوعي (نسبة الامتثال الضريبي) ***Tax Compliance Rate***	يتم قياسه بقسمة عدد الممولين الملتزمين بتقديم الإقرارات وسداد الضرائب على إجمالي عدد الممولين الملزمين. (عدد الملتزمين ضريبيًا ÷ إجمالي عدد الملزمين)
CSZ	حجم الشركة ***Company Size***	يتم قياسه باللوغاريتم الطبيعي لإجمالي الأصول في نهاية العام، أو حساب عدد الموظفين أو إجمالي الإيرادات السنوية.
CPR	ربحية الشركة ***Company Profitability***	يقاس بمعدل العائد على الأصول ويحسب من خلال (صافي ربح العام قبل الضرائب ÷ اجمالي الأصول)
TEA	نوع النشاط الاقتصادي ***Type of Economic Activity***	يقاس كمتغير وهمي يأخذ (1) اذا كان طبيعة نشاط الشركة من الأنشطة التكنولوجية المهتمة بالأمن السيبراني والقيمة (0) بخلاف ذلك
TI	البنية التحتية التقنية ***Technical Infrastructure***	يتم حصر وتصنيف التقنيات والأنظمة المستخدمة في الشركة، ثم تقييم مدى تطور البنية التحتية مقارنةً بالمعايير في الصناعة.

من أجل التخفيف من المشكلة المحتملة المتمثلة في تحيز الاختيار الذاتي والتجانس الداخلي، تم إجراء مطابقة درجة الميل (PSM). كما تم إنشاء عينة من الشركات التي تبدو في الغالب مثل الشركات النموذجية التي لا تطبق استراتيجيات الحماية، والغرض من هذا النهج هو مطابقة الأبعاد المختلفة بشكل فعال على

مستوى الشركة. يتم استخدام مطابقة زوجية لتقليل انحياز المطابقة، ويتم تقدير نموذج الاستجابة الثنائية probit للمرحلة الأولى بنفس مجموعة متغيرات التحكم مثل نموذج الانحدار الأساسي في المعادلة رقم (1)

$$TCL = \beta_0 + \beta_1\ TTC + \beta_2\ TGR + \beta_3\ TCA + \beta_4\ TCR + \beta_5\ CSZ + \beta 6\ CPR + \beta 7\ TEA + \beta 8\ TI + \varepsilon \quad \text{-------} \rightarrow (2)$$

1/5/5 نتائج الإحصائيات الوصفية

يوفر الجدول رقم (8) الإحصائيات الوصفية للمتغيرات التي تم استخدامها في المعادلة (1). المتوسط (الوسيط) لكل من ***TTC-، TGR، TCA، TCR*** هو 0.214، 0.041، 0.012، 0.011 (0.235، 0.013، 0.004، 0.000)، تشير النتائج إلى وجود تفاوت كبير، لذا يمكن ان تساعد في تحديد مجالات التحسين والتركيز على استراتيجيات لتحسين الأداء في مختلف المحالات. كما يلاحظ أن 32% من العينة لا تطبق استراتيجيات الأمن السيبراني في العام الحالي.

جدول رقم (8) نتائج الإحصاء الوصفي

3rd quartile	Median	1st quartile	S.D.	MEAN	N	*VAR*
0.35	0.235	0.006	0.182	0.214	135	***TTC***
0.167	0.013	-0.077	0.945	0.041	125	***TGR***
0.013	0.004	0	0.024	0.012	109	***TCA***
0.364	0.157	0.058	0.301	0.265	100	***TCR***
0	0	0	0.104	0.011	135	***CSS***
7.427	5.758	3.699	2.793	5.437	135	***CSZ***
3.728	2.009	1.016	13.479	2.551	135	***CPR***
0.409	0.194	0.014	1.852	0.519	135	***TEA***
0.336	0.13	0.04	0.553	0.292	135	***TI***

2/5/5 نتائج الارتباط بيرسون

يوضح الجدول رقم (9) مصفوفة ارتباط بيرسون لاختبار العلاقة بين متغيرات الدراسة وقياس مدى ملاءمة النموذج المقترح، وبهدف التحقق من وجود علاقة تأثير بين استخدام استراتيجيات الأمن السيبراني وكفاءة التحصيل الضريبي، ولتحديد قوة واتجاه هذه العلاقة في حالة وجودها، قامت الباحثة باستخدام معامل ارتباط بيرسون ومدى معنوية هذه العلاقة. كما هو موضح في الجدول التالي:

الجدول رقم (9) نتائج ارتباط بيرسون

Var.	(1) TTC	(2) TGR	(3) TCA	(4) TCR	(5) CSS	(6) CSZ	(7) CPR	(8) TEA	(9) TI
(1) TTC	1								
(2) TGR	-0.118**	1							
(3) TCA	-0.842***	-0.173**	1						
(4) TCR	0.377***	-0.002	0.196***	1					
(5) CSS	0.432***	0.002	0.012	0.114***	1				
(6) CSZ	0.302***	0.106*	0.134*	0.082*	0.873***	1			
(7) CPR	0.708***	-0.178***	-0.284***	-0.105**	-0.397***	-0.097***	1		
(8) TEA	0.208***	-0.013***	0.578***	-0.225***	-0.152***	0.345***	0.102***	1	
(9) TI	0.073***	0.344***	0.073	0.163***	0.605***	0.161***	-0.654***	-0.910***	1

* الارتباط دال عند مستوى معنوية < 10%، (.Sig < 0.1)

** الارتباط دال عند مستوى معنوية < 5%، (.Sig < 0.05)

*** الارتباط دال عند مستوى معنوية < 1%، (.Sig < 0.01)

يتضح من الجدول رقم (9) قوة العلاقة بين متغيرات الدراسة المستقلة والتابعة، وحيث أن إشارة معامل الارتباط (الموجبة) تشير إلى وجود علاقة ارتباط طردية (إيجابية)، بينما إشارة معامل الارتباط (السالبة) تشير إلى وجود علاقة ارتباط عكسية (سلبية)، وتشير قيمة معامل الارتباط إلى قوة علاقة الارتباط، يتضح للباحثة النتائج التالية:

- وجود علاقة ارتباط عكسية دالة إحصائيا بين التهرب الضريبي وكفاءة وفعالية النظام الضريبي. حيث أن معامل الارتباط سالب بقيمة (0.118) وبمستوي المعنوية (sig) أقل من (0.05)، مما يدل على وجود علاقة بين المتغيرين.

- وجود علاقة ارتباط عكسية دالة إحصائيا بين متوسط فترة التحصيل الضريبي وكفاءة وفعالية النظام الضريبي. حيث أن معامل الارتباط سالب بقيمة (0.842) وبمستوي معنوية (***sig***) أقل من (0.01).
- وجود علاقة ارتباط طردية دالة إحصائيا بين الامتثال الضريبي وكفاءة وفعالية النظام الضريبي. حيث أن معامل الارتباط سالب بقيمة (0.377) وبمستوي معنوية (***sig***) أقل من (0.01).
- وجود علاقة ارتباط طردية دالة إحصائيا بين تطبيق استراتيجيات الأمن السيبراني وكفاءة وفعالية النظام الضريبي. حيث أن معامل الارتباط سالب بقيمة (0.432) وبمستوي معنوية (***sig***) أقل من (0.05).
- وجود علاقة ارتباط طردية دالة إحصائيا بين حجم الشركة وكفاءة وفعالية النظام الضريبي. حيث أن معامل الارتباط موجب بقيمة (0.302) وبمستوي المعنوية (***sig***) أقل من (0.05).
- وجود علاقة ارتباط طردية دالة إحصائيا بين ربحية الشركة وكفاءة وفعالية النظام الضريبي. حيث أن معامل الارتباط موجب بقيمة (0.708) وبمستوي المعنوية (***sig***) أقل من (0.01).
- وجود علاقة ارتباط طردية دالة إحصائيا بين نوع النشاط الاقتصادي وكفاءة وفعالية النظام الضريبي. حيث أن معامل الارتباط موجب بقيمة (0.208) وبمستوي المعنوية (***sig***) أقل من (0.01).
- وجود علاقة ارتباط طردية دالة إحصائيا بين البنية التحتية التقنية وكفاءة وفعالية النظام الضريبي. حيث أن معامل الارتباط موجب بقيمة (0.073) وبمستوي المعنوية (***sig***) أقل من (0.01).

3/5/5 نتائج الانحدار *OLS*

يعرض الجدول رقم (10) نتائج انحدار ***OLS*** الرئيسية للعينة الكاملة المصممة لفحص الارتباط بين اتباع استراتيجيات الامن السيبراني وكفاءة التحصيل الضريبي.

جدول رقم (10) نتائج تحليل الانحدار

p-value	***t-value***	***Sta. error***	المعامل (β)	***VAR***
	3.6	0.01	0.05	($\beta 0$) المصطلح الثابت
0.000	4.5	0.04	0.21	استراتيجيات الامن السيبراني (***CSS***)
0.001	5.3	0.03	0.17	فعالية وكفاءة النظام (***TTC***)
0.002	3.4	0.02	0.14	تقليل حالات التهرب الضريبي (***TGR***)
0.003	6.2	0.01	0.13	سرعة وكفاءة التحصيل ***(TCA)***
0.053	9.2	0.05	0.16	الثقة في النظام والامتثال ***(TCR)***
0.000	7.8	0.03	0.08	حجم الشركة (***CSZ***)
0.001	4.5	0.07	0.09	ربحية الشركة (***CPR***)
0.000	6.7	0.09	0.07	نوع النشاط الاقتصادي (***TEA***)
0.002	5.5	0.08	0.11	البنية التحتية التقنية ***(TI)***
			0.92	***squares -R***
	0		23.1	***F-statistic***

يعرض الجدول السابق النتائج المستخلصة من نموذج الانحدار، والذي يهدف إلى تحديد العوامل المؤثرة على كفاءة التحصيل الضريبي. حيث تظهر نتائج تحليل الانحدار أن النموذج ذو دلالة إحصائية قوية، مع قيمة ***R-squared*** تساوي 0.92 وقيمة ***F-statistic*** تساوي 23.1 (قيمة $p < 0.001$). هذا يشير إلى أن المتغيرات المستقلة في النموذج تشرح نسبة كبيرة من التباين في المتغير التابع، وهو كفاءة التحصيل الضريبي. كما تظهر النتائج التالية:

- الحد الثابت ***(β0)***، بمعامل انحدار 0.05، خطأ معياري 0.01، والذي يمثل القيمة الافتراضية لكفاءة التحصيل عندما تكون جميع المتغيرات الأخرى تساوي صفرا.
- استراتيجيات الأمن السيبراني ***(CSS)***، بمعامل: 0.21، هذا يعني أن كل وحدة زيادة في استراتيجيات الأمن السيبراني تؤدي إلى زيادة بنسبة 21% في كفاءة التحصيل، مع دلالة إحصائية قوية (قيمة $p < 0.001$).
- فعالية وكفاءة النظام الضريبي (***TTC***)، بمعامل 0.17، هذا يعني أن كل وحدة زيادة في فعالية وكفاءة النظام الضريبي تؤدي إلى زيادة بنسبة 17% في كفاءة التحصيل، مع دلالة إحصائية قوية (قيمة $p < 0.01$).
- الثقة في النظام والامتثال الطوعي للشركات ***(TCR)***، بمعامل: 0.16، هذا يعني أن الثقة في النظام والامتثال الطوعي للشركات لها تأثير إيجابي كبير على كفاءة التحصيل، مع دلالة إحصائية (قيمة $p < 0.05$).

6 النتائج والتوجهات البحثية المستقبلية

1/6 نتائج البحث

كشفت الدراسة النظرية عن مجموعة من النتائج أهمها ما يلي:

1. توصل البحث إلى تقديم إطار نظري يوضح العلاقة بين الأمن السيبراني وكفاءة التحصيل الضريبي.
2. تقديم نموذج عملي يعتمد على استراتيجيات الأمن السيبراني لتحسين كفاءة التحصيل الضريبي وتقديم حلول واقعية للسلطات الضريبية.
3. زيادة الوعي بين المسؤولين والممارسين في القطاع الضريبي حول أهمية الأمن السيبراني وكيفية تطبيقه لتعزيز كفاءة التحصيل وضمان حماية البيانات.
4. إن تنفيذ النموذج المقترح يؤدي إلى زيادة فعالية وكفاءة تحصيل الضرائب من خلال تعزيز الحماية ضد الهجمات السيبرانية.
5. تبين أن تطبيق استراتيجيات الأمن السيبراني يعزز من أمان الأنظمة الضريبية ويقلل من المخاطر المرتبطة بالاختراقات والتهديدات السيبرانية.
6. أظهرت النتائج وجود علاقة ذات دلالة إحصائية بين استراتيجيات الأمن السيبراني وكفاءة التحصيل الضريبي، مما يشير إلى أن تطبيق استراتيجيات الأمن السيبراني يحسن فعلاً كفاءة التحصيل.
7. أثبت البحث أن استخدام استراتيجيات الأمن السيبراني يؤثر إيجابيا على حماية البيانات وتقليل الهجمات السيبرانية، مما يحسن من أمان الأنظمة الضريبية.
8. أظهرت النتائج أن تقنيات الأمن السيبراني تساهم في تحسين شفافية العمليات الضريبية وزيادة ثقة دافعي الضرائب في النظام الضريبي من خلال ضمان حماية بياناتهم وتقديم خدمات أكثر أمانًا وفعالية.
9. أثبت البحث أن تطبيق نموذج الأمن السيبراني المقترح يمكن أن يؤدي إلى تقليل الفاقد الضريبي وزيادة الإيرادات، مما يعزز فعالية جمع الضرائب.

2/6 توصيات البحث

في ضوء النتائج التي توصل إليها البحث، يمكن للباحثة تقديم بعض التوصيات التي تستهدف تعزيز كفاءة التحصيل الضريبي وحماية البيانات عبر تطوير استراتيجيات أمن سيبراني فعّالة، وتدريب الكوادر. تهدف هذه الخطوات إلى بناء نظام ضريبي آمن ومرن، يواكب المخاطر السيبرانية ويحقق استدامة الأداء الضريبي بكفاءة، ويوضح الجدول التالي رقم (11) توصيات البحث وآلية التنفيذ كما يلي:

جدول رقم (11) توصيات البحث وآلية التنفيذ

مجال التوصية	الجهة المعنية	آلية التنفيذ	الإطار الزمني والتكاليفي	صعوبات التنفيذ المحتملة	مقترحات علاجها
تطوير وتطبيق استراتيجيات قوية للأمن السيبراني في الأنظمة الضريبية	وزارة المالية بالتعاون مع وزارة الاتصالات وتكنولوجيا المعلومات "إدارة تكنولوجيا المعلومات"	تعيين فريق مختص لوضع استراتيجية شاملة للأمن السيبراني تتناسب مع أهمية البيانات الضريبية، واستخدام برمجيات حماية متطورة	يتوقع أن تتطلب هذه العملية من 6 إلى 12 شهرًا، بميزانية تتضمن تكاليف البرمجيات والمعدات وتدريب الموظفين.	نقص الكوادر المؤهلة لتنفيذ وتحديث الأنظمة، كما ان التكاليف المالية العالية قد تؤثر على تنفيذ الخطة بالكامل	عقد شراكات مع مؤسسات تقنية للحصول على الاستشارات اللازمة، وتوفير برامج تدريبية طويلة المدى لبناء كوادر مؤهلة داخليًا.
توفير برامج تدريبية لرفع مستوى الوعي بأهمية الأمن السيبراني	إدارة الموارد البشرية بالتعاون مع قسم التدريب	تنظيم ورش عمل ودورات تدريبية متخصصة في الأمن السيبراني	مدة تتراوح من شهر إلى 3 أشهر لتنفيذ البرنامج، بتكلفة تشمل أجور المدربين والمواد التدريبية	مقاومة الموظفين للتغيير أو لزيادة العبء التدريبي.	تحفيز الموظفين بمكافآت عند اجتياز البرامج بنجاح. تخصيص أوقات مرنة للتدريب لتجنب التأثير على الأداء اليومي للموظفين

مجال التوصية	الجهة المعنية	آلية التنفيذ	الإطار الزمني والتكاليفي	صعوبات التنفيذ المحتملة	مقترحات علاجها
تحديث الأنظمة الضريبية والتقنيات الأمنية دوريًا	قسم تكنولوجيا المعلومات	إعداد جدول زمني دوري لتحديث الأنظمة وتدقيقها. توظيف أدوات رصد جديدة تتابع الثغرات التقنية.	كل 6 أشهر، مع تخصيص ميزانية للصيانة الدورية.	تعقيد بعض الأنظمة القديمة الذي قد يعيق التحديث.	تخصيص ميزانية لتحديث الأنظمة القديمة إذا كانت غير قادرة على استيعاب التقنيات الجديدة.
تنفيذ اختبارات دورية لكشف الثغرات وتحسين أمان الأنظمة الضريبية	قسم تكنولوجيا المعلومات بالتعاون مع شركات متخصصة في الأمن السيبراني.	إجراء اختبارات اختراق دورية لتقييم مستوى الأمان واكتشاف ثغرات الأنظمة. استخدام برامج محاكاة للهجمات السيبرانية لمعرفة مدى استجابة الأنظمة الضريبية.	إجراء الاختبارات كل 3 أشهر، مع تخصيص ميزانية تشمل تكاليف الأدوات المتخصصة في اختبار الأمان.	التأثير على تشغيل الأنظمة الضريبية أثناء الاختبارات، مما قد يعيق سير العمل.	إجراء الاختبارات في الأوقات التي يقل فيها النشاط، مثل العطلات الرسمية، لضمان عدم تعطل العمليات الأساسية
5. وضع سياسات وإجراءات واضحة للتعامل مع الحوادث الأمنية	إدارة الأمن السيبراني بالتعاون مع جميع الإدارات ذات الصلة.	تطوير سياسات مكتوبة تتضمن خطوات الاستجابة للحوادث. إنشاء فريق طوارئ مخصص للاستجابة بأسرع وقت.	إعداد السياسات والفرق في غضون 6 أشهر، بتكلفة تتضمن التدريبات المتخصصة.	صعوبة تنسيق الاستجابة بين الإدارات المختلفة في حالة حدوث حادث كبير.	تنفيذ تمارين محاكاة للحوادث لرفع مستوى التنسيق بين الأقسام المختلفة وتوضيح الأدوار والمسؤوليات.

3/6 التوجهات البحثية المستقبلية

في ضوء نتائج الدراسة وتمشياً مع التطورات الدولية المعاصرة وارتقاءً بمهنة المحاسبة والمراجعة، يمكن للباحثة تقديم مجموعة من التوجهات البحثية المستقبلية أهمها ما يلي:

1. البحث في تقنيات جديدة ومتقدمة لتعزيز الأمان في الأنظمة الضريبية، مثل الذكاء الاصطناعي وتعلم الآلة للكشف عن التهديدات.
2. دراسة تأثير الابتكارات التكنولوجية مثل البلوك تشين والحوسبة السحابية على تحسين أمان وكفاءة التحصيل الضريبي.
3. بحث التأثيرات القانونية والتنظيمية لتطبيق استراتيجيات الأمن السيبراني في الأنظمة الضريبية وتقديم توصيات لتحسين الأطر القانونية.
4. دراسة كيفية تطبيق استراتيجيات الأمن السيبراني في دول ذات سياقات اقتصادية وثقافية مختلفة وتحليل نتائجها.
5. استكشاف كيف يؤثر الأمن السيبراني على جوانب أخرى مثل رضا العملاء وكفاءة العمليات الإدارية.
6. بحث تأثير الهجمات السيبرانية على السياسات الضريبية وكيفية تعديل السياسات لتحسين المرونة والأمان.

7 قائمـــة المـــراجـــع

1/7 المراجع العربية

1- 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***، مجلد 10، ع4، 1107 – 1183.

2- آل خليفة، مي محمد حمد عبد الله. (2023) دور التحول الرقمي في تحقيق الأمن السيبراني–دراسة تطبيقية على وزارة العدل بدولة قطر، ***مجلة البحوث الإدارية، 1-39.***

3- آل سعود، هيا بنت متعب بن ثنيان بن محمد (2024). الأمن السيبراني في بيئة الأعمال، ***مجلة المحاسبة،*** *مجلد 2، عدد 66، 24- 25.*

4- جمال الدين، هبة (2023). الأمن السيبراني والتحول في النظام الدولي، ***مجلة كلية الاقتصاد والعلوم السياسية،*** مج 24, ع1، 189 – 230.

5- خالد، وليد محمود، (2013)، الهجمات عبر الانترنت ساحة الصراع الالكتروني الجديدة، ***المركز العربي للأبحاث ودراسة السياسات***، مج 5، ع 1، ص 115- 125.

6- الرشيدي، طارق عبد العظيم، وناصر، داليا عادل عباس السيد. (2019). أثر الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية على أسعار الأسهم وأحجام التداول: دراسة مقارنة في قطاع تكنولوجيا المعلومات، ***مجلة المحاسبة والمراجعة،*** ع 2، 439 – 487.

7- السرحان، حنين عبد المهدي سالم، والمشاقبة، محمد ناصر موسى حمدان (2020). أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية في البنوك التجارية الأردنية، ***رسالة ماجستير غير منشورة***، جامعة آل البيت المفرق، 1-99.

8- شرف، إبراهيم أحمد إبراهيم. (2023). إثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبراني على قرارات المستثمرين المصريين غير المحترفين دراسة تجريبية، ***مجلة الإسكندرية للبحوث المحاسبية***، مج 7, ع1، 211 – 281.

9- شلوش، نورة (2018)، القرصنة الإلكترونية في الفضاء السيبراني، التهديد المتصاعد لأمن الدول، ***مجلة مركز بابل للدراسات الإنسانية***، جامعة بابل، المجلد8 العدد2، 185- 206.

10- الصائغ، وفاء بنت حسن، وعي افراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الالكترونية"، ***المجلة العربية للعلوم الاجتماعية***، ٢٠١٨، مج٣، ع ١٤، 18- 70.

11- الصباحي، نسرين (2017)، الحروب السيبرانية وتحديات الامن العالمي، ***المركز العربي للبحوث والدراسات، 1- 14.***

12- عرني، عبد الحكيم. (2023). تأثير الأمن السيبراني على الأعمال في التشريع المغربي، ***مجلة منازعات الأعمال***، ع76، 36 – 49.

13- علي، محمود أحمد، وعلي صالح علي صالح. (2022). أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الاستثمار بأسهم الشركات المقيدة بالبورصة المصرية: دراسة تجريبية، ***مجلة الإسكندرية للبحوث المحاسبية***، مج 6، ع 3، 1 – 48

14- علي، هيام عيد عطية محمد، دياب محمد عبد القادر، وعباس، حنان جابر حسن (2023). انعكاس دور المراجعة الداخلية في ظل أنظمة الأمن السيبراني على جودة التقارير المالية دراسة ميدانية، ***مجلة الفكر المحاسبي***، مج 27، ع 4، 121 – 162.

15- علي، هيام عيد عطية محمد، دياب، محمد عبد القادر، وعباس، حنان جابر حسن (2023). أثر دعم دور المراجعة الداخلية على تعزيز أنظمة الأمن السيبراني: دراسة ميدانية، ***مجلة الفكر المحاسبي***، مج 27، ع 4، 71 – 120.

16- عيسى، عارف محمود، ومحمد، سمير إبراهيم. (2022). قياس أثر الثالوث المظلم كسمات شخصية على اتجاهات المحاسبين نحو الإفصاح عن مخاطر الأمن السيبراني: دراسة تجريبية، ***مجلة الإسكندرية للبحوث المحاسبية***، مج6, ع3، 129- 195.

17- فريد، حنان هارون (2022). الدور المقترح لمراجع الحسابات في إضفاء الثقة على تقرير إدارة مخاطر الأمن السيبراني وأثره في دلالة القوائم المالية: دراسة تجريبية، ***المجلة العلمية للدراسات التجارية والبيئية***، مج 13، ع 4، 488 – 412.

18- اللواتي. نسرين فوزي (2017) ، التفاعل بين الانسان والحاسوب: التحدي الأكبر في العصر الرقمي، ***مجلة لغة العصر***، (4) 3 ، 123-114

19- مجلس الوزراء، المجلس الأعلى للأمن السيبراني. (2018). الاستراتيجية الوطنية للأمن السيبراني (2017- 2021). ***رئاسة مجلس الوزراء***، جمهورية مصر العربية، ٢-١٤.

20- موسى، بوسي حمدي حسن. (2023). العلاقة بين الإفصاح عن حوادث الأمن السيبراني وأتعاب المراجعة الدور المعدل لسمات منشاة المحاسبة والمراجعة دراسة تجريبية، ***مجلة البحوث المحاسبية***، 3 – 387.

21- الهلسة، تامر عيسى فائق والشيخ عماد يوسف أحمد (2021) أثر مقومات الأمن السيبراني في خصائص المعلومات المحاسبية الدور المعدل COBIT 2019 دراسة ميدانية في البنوك التجارية الأردنية، *رسالة دكتوراه غير منشورة*، جامعة العلوم الإسلامية العالمية عمان، 1- 282.

22- يعقوب، ابتهاج إسماعيل، وهاب اسعد محمد علي والفرطوسي، علي سموم (2022). مؤشر مقترح للإفصاح المحاسبي عن المخاطر السيبرانية في سوق العراق للأوراق المالية على وفق المتطلبات الدولية دراسة اختبارية، ***مجلة الدراسات المالية والمحاسبية والإدارية***، مج 9، ع 1، 1403 – 1430.

23- يوسف، أماني أحمد وهبة. (2022) واقع الإفصاح عن تقرير إدارة مخاطر الامن السيبراني وأثره على قرارات الاستثمار ومنح الائتمان في البورصة دراسة تطبيقية، ***المجلة العلمية للدراسات التجارية والبيئية***، مج 13, ع2، 109 – 28.

24- يوسف، حنان محمد إسماعيل (2024). القيمة المضافة من فعالية أداء المراجعة الداخلية لدوريها الاستشاري والتوكيدي في مجال إدارة مخاطر الأمن السيبراني دراسة انتقادية وتجريبية، ***مجلة البحوث المحاسبية***، ع1، 525 – 594.

2/7 المراجع الأجنبية

1. Ali, M. M., & Mohd Zaharon, N. F. (2022). Phishing—A Cyber Fraud: The Types, Implications and Governance. ***International Journal of Educational Reform***, 33(1), 101-121.
2. Ali, S. E. A., Lai, F.W., Dominic, P. D. D., Brown, N. J., Lowry, P. B. B., & Ali, R. F. (2021). Stock market reactions to favorable and unfavorable information security events: ***A systematic literature review***. ***Computers & Security*** *(C&S)*, vol. 110, 1- 65.
3. Alqahtani, F. H. (2017). Developing an information security policy*: A case study approach. Procedia Computer Science*, vol. 124, 691-697.
4. Asiri, M. (2022). Three essays in investment efficiency, accounting reporting complexity, and cybersecurity breaches: Evidence from corporate tax avoidance, ***Doctoral dissertation, Curtin University,*** 108-139.

5. Badawy, H. A. 2021. The Impact of Assurance Quality & Level on Cybersecurity Risk Management Program on Non-Professional Egyptian Investors' Decisions: An Experimental Study. *Alexandria* ***Journal of Accounting Research***, 5(3), 3-56.
6. Barry, T., Jona, J., & Soderstrom, N. (2022). The impact of country institutional factors on firm disclosure: Cybersecurity disclosures in Chinese cross-listed firms. ***Journal of Accounting and Public Policy,*** 41 (6), 1-23.
7. Chawla, N., & Kumar, B. (2022). E-Commerce and Consumer Protection in India: The Emerging Trend. ***Journal of Business Ethics***, 180(2), 581-604.
8. **CISA**, Cybersecurity and Infrastructure Security Agency. (2024). *Cybersecurity Reports 2024. Retrieved from [URL]*, 1-16.
9. **Deloitte**. (2020). Deloitte Cyber Risk Services: Protecting Your Business from *Cyber Threats*, 1-39.
10. **EY**. (2019). EY's Approach to Cybersecurity: *Protecting the Integrity of Financia Data, 2-26*.
11. Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. ***International Journal of Accounting Information Systems***, Vol. 38, 100- 468.
12. Hatfield, M. (2018). Cybersecurity and tax reform. **Ind. LJ,** 93, 1161.
13. Hossain, M. Z., & Johora, F. T. (2024). *Cybersecurity in Accounting*: Protecting Financial Data in the Digital Age, 1- 25.
14. **ISO/IEC** 27000 (2016). Information technology-Security Techniques-Information security management systems- Overview and vocabulary.
15. Janvrin, D., & Wang, T. (2019), Implications of cybersecurity on accounting information. ***Journal of Information Systems***, 33(3), A1-A2.
16. Jimerson, R. (2016). Avoiding online tax scams Cyber Security Tips, Volume 11, Issue 2. ***Tacoma Enterprise Information Security Program***, 1-2.
17. Juniper Research. (2015). Cybercrime will Cost Businesses Over $2 Trillion by 2019, 1-3.

18. Kamilah, A., & Khan, M. Z. K. (2021). Optimizing the implementation of beneficial ownership in transfer pricing in taxes as a corporate crime**.** ***Lex Publica***, 8(2), 47-64.
19. Kayode, O. J., Adeyinka, A. J., Adekunle, A. A., & Kayode, K. (2022). Trade-Based Money Laundering and the Era of Cybersecurity Tax Evasion in Nigeria. ***Gusau Journal of Accounting and Finance***, 3(3), V0l. 30, 205- 224.
20. Kejwang, B. (2022). Effect of cybersecurity risk management practices on performance of insurance sector: A review of literature. ***International Journal of Research in Business & Social Science*** (2147-4478), 11(6), 334-340.
21. Khamis, I. H., & Mastor, N. H. (2021). Service Quality, Tax Awareness and Tax Fairness as Determinants of Tax Compliance among E-Commerce Enterprises in Malaysia. *The International* ***Journal of Academic Research in Business and Social Sciences***, 11, 938-951.
22. Ki-Aries, D., & Faily, S. (2017). Persona- Centred Information Security Awareness. ***Computers & Security***, 70, 663-674.
23. Kim, J.-B., Li, Y., & Zhang, L. (2011). Corporate tax avoidance and stock price crash risk: Firm-level analysis**.** ***Journal of Financial Economics***, 100(3), 639-662.
24. Krivokapic, D., Nikolic, A., Stefanovic, A., & Milosavljevic, M. (2023). Financial, accounting and tax implications of ransomware attack. **Studia *Iuridica Lublinensia***, 32(1), 191-211.
25. Madani, L., Sofia, A., & Widarsono, A. (2024). The Influence of Cybersecurity Disclosure, Tax Risk, Reputation and Auditor Experience on Audit Quality. ***Jurnal Pendidikan Akuntansi & Keuangan,*** 12(2), 138-149.
26. Mittal, S., & Tyagi, S. (2020). Computational Techniques for Real-Time Credit Card Fraud Detection. In B. B. Gupta, G. M. Perez, D. P. Agrawal, & D. Gupta (Eds.), **Handbook of Computer Networks and Cyber Security**: *Principles and Paradigms* (pp. 653-681).

27. Mulyani, S., Suparno, S., & Sukmariningsih, (2023). Regulations and Compliance in Electronic Commerce Taxation Policies: Addressing Cybersecurity Challenges in the Digital Economy. *International **Journal of Cyber Criminology**,* 17(2), 133-146.
28. Palil, M. R., Amin, H. B., & Turmin, S. Z. (2020). Challenges in Implementing Taxes on E-Commerce Transactions in Malaysia**.** ***Jurnal Bisnis Dan Akuntansi,*** 22(2), 179-200.
29. Plena S., (2024), The challenge of cybersecurity for tax authorities, *(LTD)* ***Plena Solutions***.
30. PricewaterhouseCoopers (**PwC**). (2016). Turnaround and transformation in cybersecurity Key findings from The Global State of Information Security® Survey 2016, 2-17.
31. **PwC**. (2021). Cybersecurity and Privacy: PwC's Approach to Protecting Client Data, 3- 48.
32. Scarcella, L. (2020). E-commerce and effective VAT/GST enforcement: Can online platforms play a valuable role? **Computer Law & Security Review**, 36, 105- 371.
33. Securities and Exchange Commission (**SEC**). (2018). 17 CFR Parts 229 and 249. [Release Nos. 33-10459; 34-82746]. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 1-24.
34. Symantec. (2024). Symantec Internet Security Threat Report 2024. **Retrieved from [URL**], 1- 48.
35. Tantimin, T. (2021). Legal Liability of Minors as Perpetrators of Online Buying and Selling Fraud in Indonesia. ***LAW REFORM,*** 17(2), 145-156.
36. Vasarhelyi, M., 2017, Cybersecurity and Continuous Assurance, ***Journal of Emerging Technologies in Accounting****,* 14 (1): 1-12.
37. Yanto, O. (2020). Criminal Charges and Sanctions on Defamation Crime as Cyber Crime in the Information Technology Development. ***Lex Publica***, 7(2), 24-43.