أثر الإنفاق في الأمن السيبراني على الأداء في البنوك التجارية المصرية مع دراسة ميدانية

The Impact of Spending in Cybersecurity on the Performance of Egyptian Commercial Banks with A Field Study

د. عبدالعال مصطفى أبو الفضل

أستاذ المحاسبة المشارك - جامعة شقراء

أستاذ المحاسبة المساعد - المعهد العالي

للدراسات التعاونية والإدارية

مجلة الدراسات التجارية المعاصرة

كلية التجارة – جامعة كفر الشيخ

المجلد العاشر - العدد السابع عشر - الجزء الثالث

يناير ٢٠٢٤م

رابط المجلة : https://csj.journals.ekb.eg

مستخلص البحث:

يتمثل هدف البحث في التعرف على أثر الإنفاق في الأمن السيبراني على المخاطر السيبرانية، وإيجاد التأثير الوسيط للمخاطر السيبرانية في العلاقة بين الإنفاق في الأمن السيبراني والأداء في البنوك التجارية، وتم التركيز على كلاً من المنهج الاستقرائي والمنهج الاستنباطي في الإجابة على أسئلة البحث، واستخدم الباحث إستمارة استقصاء في تجميع البيانات من مجتمع الدراسة الميدانية المتمثل في مديري ونواب مديري الفروع ومدراء الأقسام والمصرفيين العاملين بالبنوك التجارية المصرية، وتم تحديد عينة عشوائية عددها (٢٢٠) مفردة من مجتمع الدراسة، وتم تجميع عدد (١٨٠) استبانة صحيحة بنسبة (٨٢%) من إجمالي الإستبانات، وأظهرت نتائج الدراسة الميدانية أن جميع المتغيرات المستقلة (الإنفاق في المنع (الوقاية) والكشف عن الجرائم السيبرانية والإنفاق في تطوير الأمن السيبراني) كان لها أثر إيجابي في تخفيض المخاطر السيبرانية في البنوك التجارية، كما أن تخفيض المخاطر السيبرانية كان له أثر إيجابي على الأداء المالي وغير المالي في البنوك التجارية، ومن حيث الأهمية النسبية لدرجة تأثير الإنفاق في الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية المصرية جاء في الترتيب الأول أثر الإنفاق في المنع (الوقاية) والكشف عن الجرائم السيبرانية في تخفيض المخاطر السيبرانية في البنوك التجارية المصرية بمتوسط (٤.٥٧)، ثم جاء في الترتيب الثاني أثر الإنفاق في تطوير الأمن السيبراني في تخفيض المخاطر السيبرانية في البنوك التجارية المصرية بمتوسط (٤.٥٤). من حيث الأهمية النسبية لدرجة تأثير المخاطر السيبرانية على الأداء المالي وغير المالي في البنوك التجارية المصرية جاء في الترتيب الأول أثر المخاطر السيبرانية على الأداء المالي في البنوك التجارية المصرية بمتوسط (٤.٨٨)، ثم جاء في الترتيب الثاني أثر المخاطر السيبرانية على الأداء غير المالي في البنوك التجارية المصرية بمتوسط (٤.٥٣)، وتم إجراء إختبار كروسكال – والاس " Kruskal-Wallis Test"وتبين عدم وجود إختلاف بين آراء فئات عينة البحث

الكلمات المفتاحية: تكلفة الأمن السيبراني، العائد على الاستثمار الأمني السيبراني، الهجمات السيبرانية، الأمن السيبرانى، المخاطر السيبرانية، الأداء المالي وغير المالي ، البنوك التجارية.

Abstract:

The research objective is to identify the impact of spending in cybersecurity on the performance of Egyptian commercial banks. It also investigates the mediating impact of cyber risks on the relationship between cybersecurity spending and performance in commercial banks. The researcher used both the inductive approach and the deductive approach to achieve the research objectives and in answering the research questions. A survey form using a self-administered questionnaire is used to collect data from banks' branch managers and deputy managers, department managers, and bankers working in Egyptian commercial banks. A random sample of (220) individuals was selected from the study population, and (180) valid questionnaires were collected, representing (82%) of the total questionnaires. The results of the field study showed that all independent variables (spending on prevention, detection of cybercrimes, and spending on developing cybersecurity) had a positive impact on reducing cyber risks in commercial banks. Reducing cyber risks also had a positive impact on the financial and non-financial performance of commercial banks, and in terms of the relative importance of the degree of impact of cyber security spending on cyber risks in Egyptian commercial banks, the impact of spending on prevention and detection of cybercrimes came in first place. In reducing cyber risks in Egyptian commercial banks with an average of (4.57). The impact of spending on developing cybersecurity in reducing cyber risks in Egyptian commercial banks is ranked as the second important variable, with an average of 4.54. In terms of the relative importance of the degree of impact of cyber risks on financial and non-financial performance in Egyptian commercial banks, the impact of cyber risks on financial performance in Egyptian commercial banks came in first place, with an average of (4.88). Then came in second place the impact of cyber risks on non-financial performance in Egyptian commercial banks with an average of (4.53). The Kruskal-Wallis Test was conducted and it was found that there was no difference between the opinions of the research sample categories

Key words: Cybersecurity cost, Return on cyber security investment, cyber security risks, financial and non-financial performance, commercial banks.

١. الإطار العام للبحث

١-١ مقدمة

تلعب الخدمات المصرفية الإلكترونية (e-banking) دورًا رئيسيًا في النمو المالي للبنوك (Sandhu & Arora,2021)، وتقدم البنوك الإلكترونية ومرافق الأجهزة الإلكترونية، مثل أجهزة الصراف الآلي (ATM)، والأكشاك الإلكترونية، والمساعد الرقمي الشخصي personal digital assistance (PDA)، والمحافظ الإلكترونية، وما إلى ذلك خدمات مصرفية أكثر ملاءمة للعميل، مما يؤدي إلى نمو مالي كبير (Soylemez & Ahmed, 2019؛ Nazaritehrani & Mashali, 2020)، ويعتبر اختراق الأمن السيبراني هو المشكلة الرئيسية للنمو المالي للخدمات المصرفية الإلكترونية، هذا وقد وظفت البنوك التجارية الأمن السيبراني لمكافحة الجرائم السيبرانية (Khalil, Usman & Manzoor, 2020)، حيث تدفع المؤسسات المالية مئات الملايين سنويًا مقابل أمنها السيبراني (Columbus, 2020).

والأمن السيبراني من الوسائل الحديثة التي تستخدم في حماية المعلومات المربوطة بشبكات الإنترنت وتكنولوجيا المعلومات، إذ يحافظ الأمن السيبراني على المعلومات من أي سرقة أو دخول غير مصرح على الأنظمة التي تخص منظمات الأعمال، وتعتبر سياسة الأمن السيبراني من السياسات الحديثة والرائدة في هذا المجال، إذ تحافظ هذه السياسة على تحقيق متطلبات السرية والمصداقية وإتاحة المعلومات في بيئة تكنولوجيا المعلومات والإتصالات، كما أن هذه السياسة تعزز جودة مخرجات نظم المعلومات، وقد ألزمت البنوك المركزية البنوك بتطبيق سياسة الأمن السيبراني ومن أهمها تثبيت برامج الحماية ضد الإختراق (صندوق النقد العربي ،2019؛ البغدادي، ٢٠٢١).

١-٢ مشكلة البحث

وفقًا لدراسة أجرتها مؤسسة كارنيجي للسلام الدولي في عام "٢٠٢٠"، فإن عدد الهجمات الإلكترونية على المؤسسات المالية يتزايد بأربعة أضعاف على أساس سنوي، كذلك بلغ متوسط تكلفة الهجمة الواحدة على القطاع المالي ٥.٧٢ ملايين دولار في عام ٢٠٢١، وذلك وفقًا لبيانات شركة "International Business Machines Corporation IBM" ومؤسسة "Ponemon"، مما يوضح أن تأمين البيانات أصبح يشكل تحديًا كبيرًا أمام القطاع المالي، وعلى الرغم من ذلك فإن معظم المؤسسات المالية لم تتخذ خطوات لتعزيز مهارات الأمن السيبراني لديها، فعلى الرغم من الإهتمام المتزايد بالمخاطر السيبرانية في الآونة الأخيرة، فإنه لا يزال هناك العديد من الدول التي لم تقم بعد بإتخاذ الإجراءات اللازمة لتفادي هذه الهجمات، فوفقًا للبيانات الصادرة عن مسح أجراه "صندوق النقد الدولي" على ٥١ دولة خلال عام ٢٠٢٣، فإن معظم المسؤولين الماليين في الدول النامية لم يستأنفوا إصدار لوائح للأمن السيبراني أو يتخذوا خطوات لإنفاذ تلك اللوائح، كما أن ٥٦% من البنوك المركزية أو السلطات الرقابية على مستوى العالم ليس لديها استراتيجية إلكترونية وطنية للقطاع المالي، وحوالي ٤٢% يفتقرون إلى نظام مخصص للأمن السيبراني أو إدارة مخاطر التكنولوجيا، وحوالي ٦٨% يفتقرون إلى وحدة مخاطر متخصصة، وما يقرب من ٦٤% لم يقوموا بإجراء إختبارات للأمن السيبراني لديهم أو تقديم الإرشادات لتعزيزه، وحوالي ٥٤% يفتقرون إلى نظام مخصص للإبلاغ عن الحوادث السيبرانية، و٤٨% ليس لديهم لوائح للجرائم الإلكترونية. https://www.youm7.com/story/2023/3/28/%6130353

وتنفق البنوك مبالغ كبيرة في الأمن السيبراني لمنع الهجمات السيبرانية، وتتكون تكاليف الأمن السيبراني من تكلفة الوقاية والكشف (PDC)، وتكلفة تطوير الأمن السيبراني (DC)، وقد أفاد الباحثون أن عددًا قليلًا جدًا من الدراسات تقيس الإرتباط بين تكلفة الأمن السيبراني والأداء للبنوك (Njoroge, 2017; Njoroge & Njeru, 2017; Odhiambo & Ngaba, 2019)، وأظهرت الدراسات إجراء عدد محدود من الدراسات حول تكلفة / الإنفاق في الأمن السيبراني والأداء المالي للبنوك التجارية (Desta, 2018)، علاوة على ذلك لا توجد دراسة في مصر على حد علم الباحث تقيس العلاقة بين تكلفة/ الإنفاق في الأمن السيبراني والمخاطر السيرانية والأداء في البنوك التجارية.

لذا يحتاج الباحثون إلى دراسة ما إذا كانت الزيادة في الإنفاق في الأمن السيبراني بسبب الضرورة الإستراتيجية تؤثر سلبا أو إيجاباً على الأداء في لبنوك، وذلك لأن هناك حاجة إلى زيادة الإنفاق على الأمن السيبراني بسبب التحول الرقمي السريع للعمليات المصرفية، وبالتالي قد يتأثر الأداء في البنوك، ويقوم هذا البحث بتحليل كيف لإستراتيجية زيادة الإنفاق في الأمن السيبراني أن تؤدي إلى تخفيض مخاطر الأمن السيبراني؟، وكيف يمكن من خلال تخفيض مخاطر الأمن السيبراني كمتغير وسيط تحسين الأداء في البنوك التجارية؟ AIG (2016), BIS (2016), Fed (2017), and EU (2018)، ومن هنا يمكن صياغة مشكلة البحث من خلال السؤال الرئيس التالي:

ما أثر الإنفاق في الأمن السيبراني على الأداء في البنوك التجارية؟

وللإجابة على السؤال الرئيس للبحث يمكن الإجابة على التساؤلات التالية:

١. كيف يمكن تقييم العائد على الإنفاق في الأمن السيبراني؟
٢. ما أثر الإنفاق في الأمن السيبراني على المخاطر السيبرانية ومن ثم على الأداء في البنوك التجارية؟

وللإجابة على هذا السؤال يلزم الإجابة على السؤالين الفرعيين التاليين:

- ما أثر تكاليف المنع والوقاية من الجرائم السيبرانية على المخاطر السيبرانية في البنوك التجارية؟
- ما أثر تكاليف تطوير الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية؟

٣. ما أثر المخاطر السيبرانية على الأداء في البنوك التجارية؟

وللإجابة على هذا السؤال يلزم الإجابة على السؤالين الفرعيين التاليين:

- ما أثر المخاطر السيبرانية على الأداء المالي في البنوك التجارية؟
- ما أثر المخاطر السيبرانية على الأداء غير المالي في البنوك التجارية؟

١-٣ هدف البحث:

يتمثل هدف البحث في التعرف على أثر الإنفاق في الأمن السيبراني على المخاطر السيبرانية، وإيجاد التأثير الوسيط للمخاطر السيبرانية في العلاقة مع تكاليف الأمن السيبراني والأداء في البنوك التجارية على الأداء في البنوك التجارية، ويتم تحقيق ذلك من خلال الأهداف التالية:

١. معرفة تقييم العائد على الإنفاق في الأمن السيبراني
٢. معرفة أثر الإنفاق في الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية.

ولتحقيق هذا الهدف يلزم تحقيق الهدفين الفرعيين التاليين:

- معرفة أثر تكاليف المنع والوقاية من الجرائم السيبرانية على المخاطر السيبرانية في البنوك التجارية.
- معرفة أثر تكاليف تطوير الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية.

٣. معرفة أثر المخاطر السيبرانية على الأداء في البنوك التجارية.

ولتحقيق هذا الهدف يلزم تحقيق الهدفين الفرعيين التاليين:

- معرفة أثر المخاطر السيبرانية على الأداء المالي في البنوك التجارية.
- معرفة أثر المخاطر السيبرانية على الأداء غير المالي في البنوك التجارية.

١-٤ أهمية الدراسة:

يعتبر البحث مهم للأكاديميين من حيث توفير المعرفة المتعمقة والمعاصرة لتأثير الإنفاق في الأمن السيبراني على المخاطر السيبرانية والأداء في البنوك التجارية مع أخذ المخاطر السيبرانية كمتغير وسيط، علاوة على ذلك تعمل هذه الدراسة على تعزيز الأدبيات في سياق تكلفة/ الإنفاق في الأمن السيراني، الأمر الذي سيكون مفيدًا للباحثين الذين يقومون بالأبحاث في هذا المجال، حيث تعتبر هذه الدراسة جديدة في سياق الإنفاق في الأمن السيبراني من خلال قياس تأثيرها على المخاطر السيبرانية وعلى الأداء في البنوك التجارية، ومن ثم فإن هذا البحث يكتسب أهميته لأنه يسهم في إلقاء الضوء على مدى تأثير الإنفاق على الأمن السيبراني على المخاطر السيبرانية والأداء في البنوك التجارية وأهمية ذلك في إتخاذ القرارات بشأن حجم الإنفاق في الامن السيبراني.

١-٥ منهج البحث:

تم التركيز على كلاً من المنهج الاستقرائي والمنهج الاستنباطي في الإجابة على أسئلة البحث، ويعتمد الباحث علي المنهج الاستنباطي لأنه يقوم على الملاحظة والاستنتاج العلمي واستقراء الواقع من خلال الدراسات السابقة المتاحة في الأبحاث العربية والأجنبية بموضوع بالدوريات العلمية ومواقع الأنترنت ذات الصلة بموضوع البحث، وذلك بهدف تكوين الإطار النظري ووضع الفروض البحثية التي يتعين إختبارها لتحقيق أهداف البحث، بينما يتم الإعتماد على المنهج الاستقرائي عند إجراء الدراسة الميدانية وذلك لإختبار فروض البحث على عينة من البنوك التجارية العاملة في مصر والتحقق من صحة أو عدم صحة فروض البحث.

١-٦ خطة البحث:

للإجابة على أسئلة البحث وتحقيقاً لأهدافه، قام الباحث بتنظيم البحث على النحو التالي:

١. الإطار العام للبحث.
٢. الدراسات السابقة.

٣. الإطار النظري للأمن السيبراني والمخاطر السيبرانية
٤. أثر الإنفاق في الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية
٥. الإنفاق في الأمن السيبراني والأداء في البنوك التجارية مع توسيط المخاطر السيبرانية.
٦. الدراسة الميدانية.
٧. نتائج البحث والتوصيات ومقترحات لبحوث مستقبلية.

٢. الدراسات السابقة:

تم تقسيم الدراسات السابقة إلى نوعين من الدراسات: دراسات تناولت مخاطر الأمن السيبراني ودراسات تناولت أثر الأمن السيبراني على أداء البنوك، وقد تم تناولهما على النحو التالي

٢-١ الدراسات السابقة التي تناولت مخاطر الأمن السيبراني:

دراسة أبو موسي (٢٠٠٤)

تعد من الدراسات الرائدة في هذا المجال في المنطقة العربية، وركزت على تحديد المخاطر الرئيسية التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في السعودية، وتمثلت أهم المخاطر في ادخال بيانات غير صحيحة وتدمير بيانات ومخرجات النظام المحاسبي وإشتراك أكثر من موظف في نفس كلمات السر وإدخال فيروسات والدخول للنظام من اشخاص غير مخولين، وتحويل المخرجات لأشخاص غير مسموح لهم بالاطلاع عليها. وخلصت إلى تحمل كثير من الشركات لخسائر مالية كبيرة بسبب اختراق نظم معلوماتها المحاسبية من قبل أطراف داخلية وخارجية. واوصت بتدعيم ضوابط الرقابة ورفع الوعي الخاص بنظم المعلومات الإلكترونية، كما أوصت باستطلاع اراء المراجعين الخارجيين والداخليين حول المخاطر الإلكترونية

دراسة الرشيدي، والسيد(٢٠١٩)

ركزت الدراسة على أثر الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية على أسعار الأسهم وأحجام التداول لشركات قطاع تكنولوجيا المعلومات المصرية ومقارنة ذلك مع الشركات الامريكية ، وخلصت الدراسة إلى ضعف الإفصاح عن مخاطر الأمن السيبراني للشركات المصرية، مما يؤثر سلبا على أسعار الأسهم وحجم التداول ومن ثم على الأداء المالي، كما تبين وجود فروق معنوية في الإفصاح عن مخاطر الأمن السيبراني بين الشركات المصرية والشركات الأمريكية، كما تبين وجود آثار إيجابية للإفصاح عن إدارة مخاطر الأمن السيبراني على أسعار الأسهم والقيمة السوقية للشركة.

دراسة على، وعلى (٢٠٢٢)

هدفت الدراسة إلى دراسة وإختبار أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الإستثمار بأسهم الشركات المقيدة بالبورصة المصرية، وكذلك إختبار أثر بعض الخصائص الديمغرافية (مستوى الخبرة والتأهيل العلمي للمستثمر) كمتغيرات مُعدّلة على العلاقة محل الدراسة. ولتحقيق هدف البحث تم إجراء دراسة تجريبية على عينة من المستثمرين بالأسهم والمحللين الماليين في شركات السمسرة، وخلصت الدراسة إلى وجود تأثير إيجابي ومعنوي لتقرير إدارة مخاطر الأمن السيبراني على قرار الإستثمار في الأسهم، كونه يضفي الثقة على أعمال الشركة في مجال

الأمن السيبراني والحماية من الهجمات الإلكترونية، مما يُمكن المستثمرين من تقييم مدى قدرة الشركة على الحفاظ على أمن المعلومات وتقليل إحتمالات حدوث إختراقات وأحداث سلبية في المستقبل، مما يُسهم في ترشيد قرارات المستثمرين وتحسين جوده أحكامهم الإستثمارية، كما خلص البحث إلى وجود تأثير معنوي لخبرة المستثمر ومستوى تأهيله العلمي على العلاقة بين الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني وقرار الإستثمار في الأسهم، كما أكدت نتائج التحليل الإضافي على أهمية الخصائص الديمغرافية للمستثمر في التأثير على أحكامه الإستثمارية.

دراسة قاسم، وإبراهيم (٢٠٢٢)

تناولت الدراسة العلاقة بين تكنولوجيا المعلومات (توافر أبعاد تكنولوجيا المعلومات، مهارات الموارد البشرية، شبكات الاتصال، قواعد البيانات) وكفاءة الابتكارات المصرفية في فروع المصارف السورية العامة في محافظة اللاذقية، وتم حساب مؤشر كفاءة الابتكارات المصرفية من خلال حساب نسبة مؤشر المخرجات إلى مؤشر المدخلات وذلك بالاعتماد على نموذج مؤشر الابتكار العالمي، ولتحقيق ذلك تم صياغة ثلاث فرضيات رئيسة، واستخدم الباحث الاستبيانة لجمع البيانات التي تم تحليلها بإستخدام الإختبارات الإحصائية: إختبار الوسط الحسابي ، وإختبار T لعينة واحدة، وإختبار الارتباط الثنائي، وتحميل الانحدار، وتوصلت الدراسة لوجود علاقة طردية جيدة بين كل من تكنولوجيا المعلومات ومؤشر المدخلات ومؤشر المخرجات، ولكن توجد علاقة عكسية ضعيفة بين تكنولوجيا المعلومات ومؤشر كفاءة الابتكار، وبالتالي لا يتم إستثمار الموارد المتاحة لدى المصارف العامة محل الدراسة بما يحقق كفاءة العمل المصرفي فيما يتعلق بتقديم الإبتكارات المصرفية وتحقيق مؤشرات الإنتاجية التي تضمن إستقرار المركز المالي في السوق المصرفية.

دراسة محروس، وصالح (٢٠٢٢)

حاولت الدراسة تطوير أداء المراجعة الداخلية في منظمات الأعمال المصرية لمواجهة مخاطر الأمن السيبراني، وذلك عن طريق إستخدام المنهجية الرشيقة Agile Approach كأحد مناهج التطوير الحديثة، بالإضافة إلى تقديم مجموعة من المقترحات توضح طريقة ومراحل تطبيق المراجعة الداخلية الرشيقة لمواجهة مخاطر الأمن السيبراني، واستكشاف مدى إستعداد منظمات الأعمال المصرية لتطبيق هذه المنهجية، وتمت الدراسة من خلال إستطلاع آراء ١٢٧ مفردة من الإدارة العليا ومسئولي تكنولوجيا المعلومات والمراجعين الداخليين في منظمات الأعمال المصرية والباحثين من أساتذة الجامعات، وبإستخدام إختبار Wallis-Kruskal توصلت الدراسة إلى عدم و جود إختلافات معنوية بين آراء فئات المستقصي منهم بشأن التزايد المستمر لمخاطر الأمن السيبراني وتأثيراته على مستوى منظمات الأعمال وعلى المستوى القومي، وعدم وجود إختلافات معنوية بين آراء فئات المستقصي منهم بشأن قصور أداء المراجعة الداخلية التقليدية في مواجهة مخاطر الأمن السيبراني وأسباب هذا القصور، بالإضافة إلى عدم وجود اختلافات معنوية بين أراء المستقصي منهم بشأن إمكانية تطوير أداء المراجعة الداخلية من خلال إستخدام المنهجية الرشيقة في مواجهة مخاطر الأمن السيبراني.

دراسة يعقوب، وآخرون (٢٠٢٢)

هدفت الدراسة إلى إقتراح مؤشر للإفصاح عن المخاطر السيبرانية ضمن المعلومات المفصح عنها في التقارير السنوية التي تصدرها الوحدات الاقتصادية، وبحكم غياب التعليمات المنظمة لهذا نوع من الإفصاحات في العراق وتراجع مركز العراق في المؤشر العالمي للأمن السيبراني إلى

المركز (١٢٩)عالميا من أصل (١٨٤) على الرغم من الإهتمام المتزايد من قبل الدولة العراقية بوضع استراتيجية للأمن السيبراني، وتوصلت الدراسة إلى بناء مؤشر للإفصاح المحاسبي عن مخاطر الأمن السيبراني وفق المتطلبات الدولية الصادرة عن الهيئات المهنية والتشريعات والأدلة الأجنبية والعربية فضلا عن الإستراتيجيات الوطنية وما قدم من قبل (AICPA) والدليل الارشادي ل(SEC) والإرشادات الرقابية المالية لبورصة تورنتو(TSX) ومعيار مجلس معايير الإستدامة (SASB)

دراسة أميرهم (٢٠٢٢)

سعت الدراسة لإختبار أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وانعكاساته على ترشيد قرارات المستثمرين، ولتحقيق هدف البحث تم إجراء دراسة ميدانية على عينة من مسئولي المراجعة الداخلية، مسئولي تكنولوجيا المعلومات، مسئولي إدارة المخاطر، المستثمرين من خلال شركات وساطة وتداول الأوراق المالية في شركات الإتصالات وقد توصلت الدراسة إلى مجموعة من النتائج النظرية والعملية لعل أهمها : لن يستطيع أصحاب المصالح وخاصة المستثمرين متابعة عمليات المخاطر السيبرانية إلا بمساعدة المراجعة الداخلية، كما أثبتت أيضا استجابات مفردات المجموعات الأربعة لعينة الدراسة نتائج الدراسة الميداني بناء على تحليل فيما يتعلق بإختبار الفرض الثاني حيث تشير النتائج إلى أنه لا توجد فروق معنوية بين آراء مسئولي المراجعة الداخلية، مسئولي تكنولوجيا المعلومات، مسئولي إدارة المخاطر، المستثمرين من خلال شركات وساطة وتداول الأوراق المالية، حيث كان مستوى المعنوية أكبر من ٠.٠٥ وبالتالي إنفاق المجموعات الأربعة على وجود عالقة بين الحد من مخاطر الأمن السيبراني وترشيد قرارات المستثمرين.

دراسة الركبان (٢٠٢٣)

هدفت الدراسة إلى التعرف على واقع تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، والكشف عن المعوقات التي تحد من تحقيقه، وكانت عينة الدراسة ٦٣ موظف وموظفة من عمادة تقنية المعلومات وإدارة الأمن السيبراني، وتم تطبيق المنهج الوصفي المسحي، وكانت الإستبانة هي أداة جمع البيانات، وتوصلت الدراسة إلى عدة نتائج منها: موافقة أفراد الدراسة بدرجة عالية وبمتوسط حسابي عام (٤,١٤) على واقع تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية، وبمتوسط حسابي عام (٢.٦٣)على المعوقات التي تحد من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية، وأيضاً بمتوسط حسابي عام (٣,٨١) على المقترحات التي تسهم في تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية.

٢-٧ الدراسات السابقة التي تناولت أثر الأمن السيبراني على أداء البنوك التجارية

دراسة Agboola (2007)

وفقًا لـدراسة Agboola تتمتع الشركات والمؤسسات المالية التي تستثمر بكثافة في المعلومات والتكنولوجيا اليوم بميزة تنافسية من حيث كونها أكثر إنتاجية، وتنمو بشكل أسرع، والمزيد من فرص الإستثمار والمزيد من الأرباح، حيث يمكن للعملاء الآن الوصول إلى خدمات بسيطة مثل الإيداع والسحب النقدي ودفع الفواتير ودفع الخدمات اليومية الأخرى من هواتفهم وأجهزة الكمبيوتر وغيرها من الأجهزة الإلكترونية التي يتم تطويرها بشكل يومي.

دراسة Njogu (2014)

حاولت الدراسة قياس تأثير نظم المعلومات الإلكترونية على ربحية البنوك التجارية الكينية للإجابة على سؤال البحث: هل تؤثر نظم المعلومات الإلكترونية على ربحية البنوك التجارية في كينيا؟ وتم جمع البيانات من مصرف كينيا المركزي والمصارف التجارية واستخدمت الدراسة تحليل الإنحدار لبيان فاعلية نظم المعلومات الإلكترونية على ربحية البنوك التجارية من خلال قياس العلاقة بين المتغير المستقل (قدرة نظام المعلومات على توفير الأمن وسلامة العمليات وسرعة الاستجابة للمتغيرات المستجدة في بيئة البنوك وتكلفة الخدمات الإلكترونية الحديثة وسرعة إنجاز المهام والمتغير التابع (معدل العائد على الأصول ومعدل العائد على حقوق الملكية) وذلك خلال الفترة من ٢٠٠٨ حتى ٢٠١٣، وتوصلت الدراسة إلى وجود علاقة إيجابية قوية بين سرعة الاستجابة للمتغيرات المستجدة في بيئة البنوك ومؤشرات الربحية ممثلة في معدل العائد على الأصول ومعدل العائد على حقوق الملكية، وأن هناك علاقة معنوية بين قدرة نظام المعلومات على توفير الأمن وسلامة العمليات وربحية البنوك.

دراسة أرشيد (٢٠١٧)

هدفت الدراسة إلى التعرف على أثر الاستثمار في تكنولوجيا المعلومات (الاستثمار في الأجهزة، والاستثمار في البرمجيات SW وعدد أجهزة الصراف الآلي)على أداء المصارف السعودية، وفقا لمقاييس الاداء، والتي تشمل العائد على الموجودات، والعائد على حقوق الملكية، اظهرت المراجعة الأدبية للدراسات ذات العالقة وجود عالقة ايجابية بين الاستثمار في تكنولوجيا المعلومات بعناصرها الثالثة والعائد على الأرباح وقد شملت الدراسة جميع المصارف السعودية المدرجة في السوق المالي السعودي خلال الفترة من ٢٠٠٦-٢٠١٢ وباستخدام الانحدار المشترك تم تحليل بيانات الدراسة التي تم الحصول عليها من موقع تداول والتقارير السنوية للمصارف السعودية وقد تم التوصل إلى وجود أثر ايجابي للاستثمار في تكنولوجيا المعلومات (الاستثمار في الأجهزة، والاستثمار في البرمجيات وعدد أجهزة الصراف الآلي) على تحسين الخدمات وزيادة الأداء المالي.

دراسة Altobishi et al. (2018)

أفاد الطوبيشي وآخرون (٢٠١٨) في دراسة تمت في الأردن أن الخدمات المصرفية الإلكترونية (الملاءمة والخصوصية والتخصيص) لها تأثير إيجابي كبير على ولاء العملاء، والذي يؤثر بدوره على النظام الأساسي للخدمات المصرفية الإلكترونية وعلى ربحية البنوك.

دراسة حسان (٢٠٢١)

تم تناول العلاقة بين الإستثمار في تكنولوجيا المعلومات والأداء المالي للبنوك في بيئات مختلفة، وتم مناقشة هذه العلاقة بإستعراض أهم الدراسات الأجنبية والعربية ذات الصلة بالموضوع، كما حاولت التعرف على أثر تكنولوجيا المعلومات والإتصالات على أرباح ومخاطر الصناعة المصرفية في الاتحاد الأوروبي، وبشكل أدق تبحث الدراسة في أثر الإستثمار في التكنولوجيا وانتشارها على ربحية البنوك وإستقرارها في ٢٨ دولة أوروبية، وقد تم جمع البيانات بالاعتماد على مؤشرات التنمية العالمية والتابعة للبنك الدولي وذلك خال الفترة من ١٩٩٥-٢٠١٥ وبعد إجراء التحليل توصلت الدراسة إلى وجود دور كبير وإيجابي للإستثمار في تكنولوجيا المعلومات على تحسين الأداء بالبنوك العاملة في أوروبا.

دراسة Bokhari & Manzoor (2022)

ركزت الدراسة على أثر تطبيق معيار ISO27001 (متطلبات نظام إدارة أمن المعلومات الفعال) على الأداء المالي وتحسين السمعة التجارية، وخلصتالدراسة إلى أن إنخفاض الوعي لدي العاملين والمديرين يمثل العائق الرئيسي لتطبيق إدارة فعالة لمخاطر أمن المعلومات، حيث يفضل اغلب المديرين الأساليب العلاجية وليس الوقائية مما يزيد من تكلفة الأضرار، كما قدمت دليل تطبيقي يؤكد تحسن الأداء المالي للبنوك بإستخدام معدل العائد على الأصول ومعدل العائد على حقوق الملكية، وتبين أن البنوك التي طبقت أنظمة قوية لأمن المعلومات تمتعت بأداء مالي قوي وتحسين السمعة التجارية.

دراسة رشوان، وقاسم (٢٠٢٢)

تناولت الدراسة أثر إدارة مخاطر الأمن السيبراني على دعم وتعزيز الاستقرار والشمول المالي في البنوك الفلسطينية، حيث تدرك البنوك خطورة الاختراقات السيبرانية على الاستقرار، وخلصت إلى وجود دور هام للاستقرار والشمول المالي للبنوك في زيادة رفاهية العملاء والمجتمع من خلال تخفيض تكلفة الخدمات وتحسين الأداء المالي، كما خلصت لوجود أثر معنوي لإدارة مخاطر الأمن السيبراني على دعم وتعزيز الاستقرار والشمول المالي في البنوك الفلسطينية، كما تعتمد البنوك على الإجراءات الواردة في المعايير الدولية لإدارة مخاطر الأمن السيبراني .وأوصت بإستخدام النماذج الفعالة لإدارة المخاطر السيبرانية التي تهدد الاستقرار المالي في البنوك.

دراسة Gatzert & Schubert (2022)

بينت الدراسة علاقة إدارة المخاطر الإلكترونية في البنوك وشركات التأمين الأمريكية بالوعي وأثره على الأداء المالي، من خلال الإفصاح عن معلومات إدارة المخاطر السيبرانية في التقارير السنوية للشركات الكبيرة والمتوسطة، وخلصت الدراسة إلى وعي العاملين بشركات التأمين بالمخاطر الإلكترونية، وتوصلت لوجود علاقة معنوية طردية بين إدارة المخاطر الإلكترونية وقيمة الشركة مقاسة بواسطة Tobin Q مما يؤثر إيجابا على الأداء المالي.

٧-٣ نتائج الدراسات السابقة:

من خلال إستعراض الدراسات السابقة تم التوصل إلى ما يلي:

- حظي موضوع الأمن السيبراني ومخاطر الأمن السيبراني بمساحة كبيرة من الدراسات والأبحاث في مجالات عديدة.
- اعتمدت بعض الدراسات على التحليل النظري للدراسات السابقة، واعتمد البعض الأخر على إستخدام التحليل الإحصائي لعدد من البيانات الفعلية للتوصل إلى إستنتاجات فيما يتعلق بكل من المخاطر السيبرانية والأمن السيبراني.
- تناولت العديد من الدراسات أثر الاستثمار في تكنولوجيا المعلومات على الأداء في البنوك التجارية وكانت مكونات الإستثمار في تكنولوجيا المعلومات التي تعرضت له تلك الدراسات في أجهزة الصراف الآلي، الخدمات المصرفية عبر الهاتف المحمول، الخدمات المصرفية عبر الإنترنت، بطاقات الخصم والائتمان وغيرها.
- ندرة الدراسات التي تناولت علاقة الأمن السيبراني بالمخاطر السيبرانية والأداء في البنوك التجارية.

- لم تتناول الدراسات السابقة على حد علم الباحث أثر الإنفاق في الأمن السيبراني على المخاطر السيبرانية والأداء في البنوك التجارية.

٧-٤ ما يميز الدراسة الحالية عن الدراسات السابقة:

من إستعراض وتحليل الدراسات السابقة يتضح تتناول المخاطر السيبرانية وتأثير الجرائم الإلكترونية على البنوك بشكل عام، ولم توضح الدراسات السابقة التكاليف التي يتعين على البنوك أخذها في الاعتبار عند الإنفاق في الأمن السيبراني لمنع أو الحد من الهجمات السيبرانية، ولعدم وجود دراسات تناولت أثر الإنفاق في الأمن السيبراني على أداء البنوك التجارية في ظل توسيط متغير المخاطر السيبرانية، يسعى البحث لسد هذه الفجوة البحثية، وفتح المجال للباحثين في هذا الموضوع الهام لتناوله من أبعاد أخرى.

٧-٥ فروض البحث:

يسعى البحث إلى إختبار الفروض التالية:

الفرض الرئيس الأول: يؤثر الإنفاق في الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية.

وينقسم الفرض الرئيس الأول إلي فرضين فرعين هما:

١. تؤثر تكلفة المنع والكشف عن الجرائم السيبرانية على المخاطر السيبرانية في البنوك التجارية.

٢. تؤثر تكلفة تطوير الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية.

الفرض الرئيس الثاني: تؤثر المخاطر السيبرانية على الأداء المالي وغير المالي في البنوك التجارية.

وينقسم الفرض الرئيس الثاني الي فرضين فرعين:

٣. توثر المخاطر السيبرانية على الأداء المالي في البنوك الإلكترونية.

٤. توثر المخاطر السيبرانية على الأداء غير المالي في البنوك الإلكترونية.

٣. الإطار النظري للأمن السيبراني والمخاطر السيبرانية:

سيتم تناول الإطار النظري لكل من الأمن السيبراني والمخاطر السيبرانية على النحو التالي:

٣-١ الأمن السيبراني:

سيتم في هذا الجزء تناول كلُ من مفهوم وخصائص ومحاور وأنواع وفوائد الأمن السيبراني على النحو التالي:

٣-١ -١ مفهوم الأمن السيبراني:

يهتم الأمن السيبراني بتصميم وتطبيق التقنيات والعمليات والضوابط والممارسات اللازمة لحماية الأنظمة والشبكات والبرامج والأجهزة والبيانات من التعرض للهجمات والتهديدات الإلكترونية والفيروسات وسد ثغرات نقاط الضعف المباشرة أو غير المباشرة، ويتم ذلك من خلال مجموعة من الإجراءات منها القيام بهجوم تجريبي متعمد لاكتشاف الثغرات والعمل على إصلاحها، وتصميم مجموعة من إجراءات الاستجابة والتخفيف من الآثار الناتجة عن التعرض للخطر أو التلف أو الوصول غير المرخص به، حيث يسعى المخترق للتلاعب بالنظام الرقمي للضحية والسيطرة عليه بصورة غير قانونية بإستخدام أجهزة متطورة أو إستغلال ثغرات النظام، أو انخفاض الوعي التكنولوجي للمستخدم (على، وصالح، ٢٠٢٢).

ويعبر مفهوم الأمن السيبراني لأنظمة المحاسبة عن درجة الحماية والتأمين لإدارة العمليات المحاسبية من خلال توفير تقنيات وبرمجيات مناسبة بما يضمن منع الإختراق السيبراني الداخلي والخارجي للبيانات والمعلومات والأنظمة والأجهزة والبرمجيات والعمليات المحاسبية، وتتم الحماية بإستخدام الدرع السيبراني كجدار حماية فعال لاكتشاف الثغرات (Alqahtani, F. H. (2017)، كما أن الأمن السيبراني هو ممارسة تأمين أنظمة وشبكات الكمبيوتر ضد الوصول غير المصرح به، عن طريق التخفيف من مخاطر المعلومات ونقاط الضعف، وبالتالي باتت هذه الممارسة جزءًا أساسيًا من الحفاظ على سلامة الشركات والمستخدمين الأفرادhttps://cutt.us/6H4AY . ويرى الباحث أن الأمن السيبراني يتعلق بتأمين أنظمة وشبكات الكمبيوتر من خلال تكنولوجيا المعلومات والاتصالات من التعرض للهجمات والتهديدات الإلكترونية والفيروسات وسد ثغرات نقاط الضعف المباشرة أو غير المباشرة.

٣-١-٢ خصائص الأمن السيبراني:

تتعدد خصائص الأمن السيبراني ومن أهمها (Kejwang, 2022 ; Alqahtani, F. H. (,2017):

١. الثقة وعدم الثقة: حيث يتعامل الأمن السيبراني مع كل البرامج والتقنيات والروابط وغيرها على أنها غير جديرة بالثقة، وبالتالي يسمح فقط بمرور الموثوق منها ويمنع مرور الخبيث.
٢. الحماية من التهديدات الداخلية الناتجة عن إنخفاض وعي المستخدم أو جهله بأمن المعلومات، بتنبيه الموظفين بالخطر لمنع حدوث الاختراق، حيث تبين أن أخطر التهديدات السيبرانية تنشأ بسبب إنخفاض وعي الموظفين مما يضر بسمعة الشركات.
٣. الحماية من التهديدات الخارجية من خلال بناء جدار حماية يعمل على مدار الساعة كمرشح إلكتروني للبرامج والتقنيات لتصفية المخاطر الرقمية الخارجية، ومعالجة الثغرات التي قد يستغلها طرف ثالث للسيطرة والتحكم.
٤. تحقيق رؤية شاملة على نقاط القوة والضعف والثغرات التكنولوجية المحتملة التي تؤثر على الأداء المالي والقرارات الاقتصادية لمستخدمي المعلومات، والعمل على حلها بأسرع وقت، وتقديم مقترحات تمنع تكرارها.

٣-١-٣ محاور سياسية الأمن السيبراني

تتعدد محاور سياسة الأمن السيبراني، ومن أهمها: (عباس، ٢٠١٠ ;https://2u.pw/qui5BA2https://2u.pw/tWkeENZ)

١. تحديد الأدوار والمسؤوليات بما في ذلك مسؤولية إتخاذ القرار داخل الشركة فيما يتعلق بإدارة المخاطر السيبرانية وبما يشمل حالات الطوارئ والأزمات.
٢. إدارة المعلومات وتتضمن حوكمة البيانات وتصنيفها بالإضافة إلى أمن وإدارة المعلومات وبيئة تكنولوجيا المعلومات والإتصالات في الشركة، بهدف حماية البيانات أثناء عملية الإعداد والنقل والعزل والإتلاف، وإحكام عملية الرقابة على جميع الموارد المعلوماتية الإلكترونية وغير الإلكترونية، بالإضافة إلى تحقيق الأمن والحماية اللازمة للمعلومات من الوصول أو الاستعمال غير المرخص أو الافصاح عن موارد المعلومات في المنظمة.
٣. خصوصية بيانات العملاء: وتهدف هذه السياسة إلى الحفا ظ على المعلومات التي تتعلق بالعملاء وعدم الإفصاح عنها إلى جهات خارجية، وكذلك مراعاة عدم إنتهاك خصوصية المعلومات من قبل موظفين آخرين لا علاقة لهم بالمعلومات.
٤. إدارة المخاطر السيبرانية بالإضافة ضوابط الحماية للحد من والسيطرة على المخاطر السيبرانية وإلى خطط الإستمرارية والتعافي من الكوارث.
٥. تحديد آلية الافصاح للأطراف المعنية عن بنود سياسة الأمن السيبراني.
٦. تحديد الجهة المالكة ونطاق التطبيق ودورية المراجعة والتحديث وصلاحيات الإطلاع والتوزيع والأهداف والمسؤوليات وإجراءات العمل المتعلقة بها والعقوبات في حال عدم الإمتثال وآليات فحص الإمتثال.

٣-١-٤ أنواع الأمن السيبراني:

هناك عدة أنواع مختلفة من الأمن السيبراني تتمثل فيما يلي :https://2u.pw/c5zCUHL

النوع الأول: أمن الشبكاتNetwork Security

تحدث أغلب الهجمات الإلكترونية من خلال الشبكات الالكترونية، لذا يجب أن يكون هناك حل لتلك المشكلة، ومن أفضل الحلول الاعتماد على الأمن السيبراني حيث أنه يساعد على حماية كافة شبكات الحاسب من الهجمات.

النوع الثاني: الأمن السحابيCloud Security

في الفترة الأخيرة تم الإعتماد على الذكاء الاصطناعي سواء من قبل الأفراد أو من قبل الشركات والهدف من ذلك هو التحسين من جودة العمل وإنجاز الكثير من المهام والتعزيز من تجربة العملا، فمن المعروف أن كم البيانات التي يتم تخزينها من الصعب أن يتم الإحتفاظ بها لذلك هناك العديد من الشركات المختلفة تعمل على توفير أفضل الخدمات التي تساعد على حل تلك المشكلة في وقت قياسي وهنا من أفضل تلك الخدمات(Microsoft Azure) (Google Cloud) .

النوع الثالث: أمن التطبيقات

يعد هذا النوع من أحد أنواع الأمن السيبراني، فمن المعروف أن تطبيقات الويب يتم إتصالها بالانترنت، لذا قد يتم إختراقها وسرقة البيانات وهنا في حال التساؤل عن ما أهمية الأمن

السيبراني فهذا النوع يساعد الشركات من حماية البيانات من أي هجمة مثل (الفيروسات – تشفير المعلومات) وغيرها.

النوع الرابع: الأمن التشغيلي

إذا تعرضت البيانات إلى الاختراق يساعد هذا النوع على الوصول إلى العديد من الخطط البديلة، لذلك يتم الإعتماد عليه في أغلب الشركات والمؤسسات الضخمة.

٣-١-٥ فوائد الأمن السيبراني:

تتعدد فوائد الأمن السيبراني أهميته وتتمثل فوائد الأمن السيبراني في العديد من النقاط التي نوضحها فيما يلي https://cutt.us/6H4AY :

١. حماية سُمعة الأعمال: تسعى جميع المؤسسات لكسب ثقة عملائها وتعزيز سُمعتها وعلامتها التجارية في السوق، وهو ما لن يتحقق إلا بتطبيق إستراتيجية الأمن السيبراني، التي توفر الأمان الكامل للبيانات، وعدم وقوع إنتكاسة مفاجئة، وعندما تكتسب الشركة تاريخًا في حماية بيانات الأعمال والعملاء تزداد قاعدة عملائها.
٢. حماية البيانات الشخصية: لا تقتصر الحماية التي يوفرها الأمن السيبراني على بيانات الشركات فقط؛ بل يشمل أيضًا البيانات الشخصية للموظفين والعملاء، إذ يمكن للأمن السيبراني أيضًا حماية البيانات من التهديدات الداخلية، سواء كانت عرضية أو بنية خبيثة، كما يضمن إمكانية وصول الموظفين إلى الإنترنت وإستخدامه في العمل دون تهديدات بخرق البيانات.
٣. تعزيز الإنتاجية: تؤدي الهجمات والجرائم الإلكترونية إلى خرق البيانات، وهو ما يؤثر على سير العمل والشبكات والأداء، وبالتالي تتأثر الإنتاجية بالسلب، وتتوقف الشركة المتضررة عن العمل، ولذلك فإن من أبرز فوائد الأمن السيبراني تعزيز إنتاجية الأفراد والشركات من خلال مسح الفيروسات، وتحسين جدران الحماية، والنسخ الاحتياطية الآلية.
٤. تعزيز الوضع السيبراني: الأمن السيبراني يوفر للشركات حماية رقمية شاملة، وهو ما يمنح الموظفين المرونة والأمان والحرية للوصول إلى الإنترنت، فهذه الإستراتيجية تُمكن الشركات من التصرف والإستجابة أثناء وبعد الهجوم الإلكتروني.
٥. تحسين إدارة البيانات: قيام المنظمات برصد بياناتها بصورة مستمرة من خلال تنفيذ إستراتيجيات الأمن السيبراني، يضمن تنفيذ لوائح أمن البيانات بشكل مثالي لتلك البيانات التي تمثل جوهر المنتجات وإستراتيجيات التسويق.
٦. زيادة تثقيف القوى العاملة: من ضمن إستراتيجيات الأمن السيبراني تثقيف الموظفين والعاملين في الشركات حول المخاطر المحتملة مثل برامج الفدية وبرامج التجسس وخروقات البيانات وغير ذلك من العمليات اليومية للمؤسسة، فعند تثقيف الموظف حول تلك المخاطر سيصبح أكثر وعيًا قبل النقر فوق الروابط الضارة أو الملفات المشبوهة، كما سيتمكن من معرفة الإجراء الصحيح في حالة حدوث أي خطأ.
٧. حماية المواقع الإلكترونية: تعتمد غالبية الشركات على المواقع الإلكترونية في التسويق لمنتجاتها وخدماتها، وبالتالي فإن تعطل تلك المواقع يؤدي إلى خسارة الإيرادات، وفقدان المعاملات والإتصالات، وتدهور ثقة العملاء، ولذلك، فإن تنفيذ عملية الأمن السيبراني

يضمن حماية تلك المواقع من الضرر غير المتوقع، ومن ثم وصول العملاء إليها على المدى الطويل.

٨. تقليل الخسائر المالية: تساعد تدابير الأمن السيبراني في تقليل الخسائر المالية للأفراد والشركات والمنظمات، تلك الخسائر التي تسببها الهجمات الإلكترونية، إذ يؤدي تنفيذ استراتيجية الأمن السيبراني بشكل فعال إلى تقليل احتمالية حدوث هجوم إلكتروني ناجح وتقليل الخسائر المالية الناجمة، ومن تلك التدابير: إستخدام كلمات مرور قوية، وتحديث البرامج والأنظمة بانتظام، وزيادة وعي الموظفين حول كيفية تحديد وتجنب التهديدات الإلكترونية المحتملة.

٩. حماية الملكية الفكرية: تشمل الملكية الفكرية أصولًا ذات قيمة مثل الأسرار التجارية وبراءات الإختراع وحقوق التأليف والنشر والعلامات التجارية، تلك الأصول التي لا غنى عنها بالنسبة للشركات للحفاظ على مكانتها وسط الشركات المنافسة، ولذلك فإن من أهم مميزات الأمن السيبراني حماية الملكية الفكرية من خلال منع التزييف، تأمين براءات الاختراع، حماية الأسرار التجارية، حماية حقوق التأليف والنشر.

١٠. حماية الهوية والموارد المالية من السرقة: تُعد سرقة الهوية والموارد المالية من أكثر الجرائم الإلكترونية شيوعًا، إذ يستطيع المخترقون الوصول إلى المعلومات الشخصية وفتح حسابات جديدة باسم الضحية، كما تتضمن الهجمات الإلكترونية إختراق الحسابات المصرفية أو إستخدام البرامج الضارة لسرقة أرقام البطاقات الائتمانية، وإجراء عمليات الشراء بإسم الضحية، ومن ثم تراكم الديون عليه وبالتالي يوفر الأمن السيبراني الحماية اللازمة للهوية من السرقة.

١١. الإمتثال للوائح: التزام الشركات والمؤسسات بمعايير ولوائح الأمن السيبراني يحميها من المشكلات القانونية والغرامات المُحتملة.

١٢. ضمان أمن العمل عن بُعد: أصبح تنفيذ تدابير الأمن السيبراني أمرًا ضروريًا في ظل شيوع العمل عن بُعد بشكل متزايد خلال السنوات الأخيرة، لأنه يضمن الوصول الآمن إلى الموارد التنظيمية وإستخدامها، والحفاظ على الإنتاجية مع تقليل المخاطر المرتبطة ببيئات العمل عن بُعد.

٣-٢ المخاطر السيبرانية:

يشير مفهوم مخاطر الأمن السيبراني على انه المخاطر التشغيلية لأصول المعلومات والتقنية التي تؤثر على سرية أو توافر أو سلامة المعلومات او الأنظمة. (Kumar, Thomas, 2022)، وأن المخاطر التي تشكلها البرامج الضارة المدمرة وسرقة البيانات وهوية العميل والتلاعب بها بإعتبارها تهديدات إلكترونية تؤثر على أعمال البنوك وبنيتها التحتية المالية (Piotrowski, 2022)، وأكدت دراسة (بانقا، ٢٠١٩) أنه على الرغم من أهمية التقنيات الحديثة في نظم المعلومات والتكنولوجيا الرقمية، مثل "إنترنت الأشياء" وسلسلة الكتل اللامركزية وخدمات الحوسبة السحابية في بيئة الأعمال إلا أنها تشكل تحدياً كبيراً للأمن الإلكتروني حيث زادت كثافة وخطورة الهجمات الإلكترونية في الآونة الأخيرة، مما يترتب عليه تعطيل المعاملات المالية والإنتاجية، وزيادة معدلات الربحية الخبيثة والرسائل الإلكترونية الضارة.

وقد أشار صندوق النقد الدولي إلى أن أدوات القرصنة قد أصبحت الآن أقل تكلفة وأكثر سهولة وأشد قوة، مما يتيح للقراصنة ذوي المهارات المحدودة إلحاق ضرر أكبر مقابل نسبة ضئيلة من

التكلفة السابقة، ويؤدي التوسع في الخدمات القائمة على الأجهزة المحمولة (المنصة التكنولوجية الوحيدة المتاحة للكثيرين) إلى زيادة فرص القرصنة، ويستهدف المهاجمون المؤسسات الكبيرة والصغيرة على حد سواء ويعملون عبر الحدود، ولذلك يجب أن تكون محاربة الجريمة السيبرانية والحد من مخارطها مسؤولية مشتركة للجميع.

٣-٢-١ أنواع المخاطر السيبرانية:

مع التطور التكنولوجي الذي تشهده بيئة الأعمال قد تتعرض المؤسسات والمنظمات لمخاطر عديدة في مجال أمن المعلومات والسيبرانية ويمكن تصنيف هذه المخاطر إلى عدة أنواع، منها (بانقا، ٢٠١٩؛ شحاتة، ٢٠٢٢)

١. الاختراقات السيبرانية: وهي مخاطر تتعلق بالتعرض للهجمات السيبرانية التي تستهدف استغلال ثغرات الأمن في الأنظمة والشبكات الإلكترونية، والتي يمكن أن تؤدي إلى تسريب المعلومات الحساسة والبيانات الشخصية، وتعريض الشركات والمؤسسات للفقدان المالي والسمعة السيئة.
٢. الاحتيال الإلكتروني: وهي مخاطر تتعلق بالتعرض لعمليات الاحتيال والتزوير عبر الإنترنت، والتي يمكن أن تستهدف المؤسسات والأفراد على حد سواء، مثل الرسائل الاحتيالية والبريد الإلكتروني المزور ولتصيد الاحتيالي.
٣. البرمجيات الخبيثة: وهي مخاطر تتعلق بتعرض الأنظمة الإلكترونية للعدوى بالبرمجيات الخبيثة، والتي يمكن أن تؤدي إلى فقدان البيانات والمعلومات الحساسة، وتعطيل الخدمات والعمليات الحيوية في المؤسسات والشركات.
٤. الاختراقات الداخلية: وهي مخاطر تتعلق بالتعرض للهجمات من قبل الموظفين أو الأشخاص المرتبطين بالمؤسسة من الداخل، والتي يمكن أن تؤدي إلى تسريب المعلومات والبيانات الحساسة والمصادر المالية، وتعريض الشركة للفقدان المالي والسمعة السيئة.
٥. النقص في الأمان والحماية: وهي مخاطر تتعلق بعدم وجود التدابير الأمنية الكافية في الأنظمة الإلكترونية والشبكات والتطبيقات والبرامج، والتي يمكن أن تؤدي إلى تعرض المؤسسات للتهديدات السيبرانية والاختراقات والاحتيال الإلكتروني، وهذا يتطلب توفير تدابير أمنية متعددة وفعالة، مثل تحديث البرامج والأنظمة الإلكترونية بانتظام، وتطبيق إجراءات الحماية والتشفير لحماية المعلومات والبيانات الحساسة، وتدريب الموظفين على أسس الأمن السيبراني والوقاية من الهجمات الإلكترونية.

ويتطلب تحديد هذه المخاطر والتعامل معها وجود إستراتيجيات وسياسات أمنية فعالة ومتكاملة، والتي يتم تطبيقها على المستويات المختلفة في المؤسسة، وتحديد الأدوات والتقنيات اللازمة لتطبيقها ومراقبتها بانتظام، كما يتطلب التعامل مع هذه المخاطر الحصول على دعم الإدارة العليا وتوفير الموارد اللازمة لتحقيق أهداف أمن المعلومات والسيبرانية في المؤسسات المالية.

٣-٢-٢ حتمية مخاطر الأمن السيبراني

ليس من السهل تحديد الإنفاق الأمثل في البنية التحتية للأمن السيبراني التي يمكن أن تحد من نمو الجرائم السيبرانية (Eling & Lehmann, 2018)، حيث لا يوجد نظام مثالي ضد الخروقات السيبرانية، وأيضًا بسبب مشكلة الخطر الأخلاقي (Vagle, 2020)، قد يترك الخبراء الفنيون الذين

يقدمون حلول الأمن السيبراني عيوبًا في الأنظمة في غياب المراقبة التنظيمية الكافية لتطوير البرمجيات وترقيتها والحفاظ على المعايير الأخلاقية من قبل المبرمجين، ولذلك فإن إختراق نظام الأمن السيبراني أمر لا مفر منه لأن بعض الثغرات غير المعروفة في النظام موجودة دائمًا بغض النظر عن التطور التكنولوجي، فعلى سبيل المثال لا يتطلب الإتصال بين جهازين عادةً مصادقة يدوية أخرى عندما يظلان متصلين بسلاسة، وهذا يعني أن أي شخص يتسلل إلى الشبكة يمكنه إرسال رسالة كاذبة مقنعة (Moore, 2010)، وتعد السرقة الإلكترونية من حساب بنك بنغلاديش مثالًا جيدًا، فقد أطلق الاحتياطي الفيدرالي الأمريكي ٨١ مليون دولار للمتسللين الذين أرسلوا رسائل SWIFT مزيفة متنكرة لتحويل الأموال من حساب بنك بنغلاديش (Page et al., 2017).

أما عن مخاطر الأمن السيبراني في القطاع المصرفي فوفقاً لسيناريوهات تراكم المخاطر Scenarios Accumulation Riskالتي طورتها Swiss Re، فإن القطاع المصرفي هو الأكثر تعرضاً للتهديدات، يليه المراكز الطبية ثم قطاع التأمين ،وتتمثل المخاطر السيبرانية في القطاع المالي بالتالي (نشرة الاتحاد المصري للتأمين، ٢٠١٩ :٣)

١. فقدان أو سرقة البيانات Theft or Loss of Data البيانات الشخصية والبيانات التجارية، وأي بيانات ذات قيمة بالسوق السوداء تعتبر خطر (الدافع: المكاسب المالية أو التنافسية).

٢. تدمير البياناتData Destruction مسح البيانات الالكترونية أو تشفيرها أو منع الوصول إليها (الدافع: والابتزاز، والإرهاب، أو الحرب).

٣. إنقطاع الإتصالاتDisruptions Communication تعطيل الموقع الالكتروني أو تعطيل الشبكة؛ تشويه الموقع؛ الاستيلاء على صفحات وسائل التواصل الإجتماعي (الدافع: الإيديولوجية، والابتزاز، والإرهاب).

٤. سرقة الأموال والأوراق المالية والصناديق وغيرها، Securities ,Monies of Theft Funds, etc إلكترونياً ما وراء سرقة البيانات: المال والأوراق المالية هي هدف عالي القيمة سواء مادياً(الدافع: المال).

وبما أن نظام الأمن القائم على تكنولوجيا المعلومات ينطوي على مخاطر متأصلة يصعب حلها، فإن الممارسين يحولون تركيزهم نحو إدارة المخاطر السيبرانية لتقليل التأثير (Geyres & Orozco, 2016). وبالتالي، يحتاج المديرون إلى التفكير في الإنفاق الأمثل على التكنولوجيا السيبرانية.

٤. أثر الإنفاق في الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية

بما أن مخاطر الأمن السيبراني تؤدي إلى مخاطر نظامية، وعيه تجد المؤسسات المالية أن إنفاقها في الأجهزة والبرمجيات وصيانة الأنظمة عالية الجودة وتدريب القوى العاملة أمر لا غنى عنه لتطوير بنية تحتية تشغيلية أكثر مرونة، ولذلك يرى الباحثون أن البنوك تتكبد المزيد من النفقات العامة الثابتة التي يمكن أن تؤثر على صافي الأرباح (Keswani & Kumar, 2015)، وفي هذا الصدد، يحلل (Eling & Lehmann, 2018) أن تقييم الخسائر غير الملموسة لفشل الأمن السيبراني أمر معقد نظرًا لأن تآكل ثقة العملاء في قدرة البنوك على حماية أموالهم ومعلوماتهم السرية كان من الممكن أن يؤدي إلى تداعيات خطيرة، وأيضًا في حالة وقوع هجمات إلكترونية قد يتم تكبد بعض الخسائر بسبب إحتمال رفع دعاوى قضائية ومطالبات تعويض من قبل العملاء

المتضررين أو أطراف خارجية أخرى (Kopp et al., 2017)، وهذا يعني أن البنوك بحاجة إلى تحليل الفوائد والتكاليف والخسائر قبل تخصيص ميزانية للإنفاق في التكنولوجيا السيبرانية (Toivanen, 2015)، ومع ذلك من الناحية العملية تحتفظ البنوك بمخصصات الميزانية للحصول على التكنولوجيا اللازمة دون تحليل صافي القيمة الحالية (Gordon & Loeb, 2002b)، وبالتالي تنفق البنوك في كثير من الأحيان أكثر من المطلوب على النحو الأمثل وتؤثر على الأرباح (Gordon & Loeb, 2002a)، ويؤدي هذا النوع من الأبحاث إلى مسألة محيرة لمديري البنوك عندما يقررون ما إذا كانت الزيادة الهامشية في الإنفاق على الأمن السيبراني يمكن أن تؤدي إلى قيمة مضافة متناسبة أكبر(CarlColwill, 2009; Trautman & Altenbaumer 2010)، وسيتم تناول أثر الإنفاق في الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية على النحو التالي:

٤-١ الإنفاق في الأمن السيبراني

تعمل البنوك والمؤسسات المالية على زيادة نفقاتها التكنولوجية بشكل مستمر للتغلب على التهديدات السيبرانية المتزايدة التي تزيد من تكاليف التشغيل الثابتة (Euromoney, 2017). ويظهر تقرير ديلويت أن نفقات التكنولوجيا للبنوك (كنسبة من إجمالي الإيرادات) ترتفع إلى ٧.١٦%، وهي الأعلى بين جميع قطاعات الاقتصاد العالمي (Kark et al., 2017). ولذلك فإنه يشير إلى أن الصناعة المالية العالمية تتأثر سلبًا بكل من الخسائر المباشرة الناجمة عن إنتهاكات الأمن السيبراني والتكاليف العامة السيبرانية الإضافية، وبشكل عام فإن مجموعة الأدبيات التي تم تطويرها تحمل بشكل عام إجماعًا على أن المؤسسات تتحمل عبئًا ماليًا إضافيًا ناتجًا عن الحوادث السيبرانية المتفشية التي تحدث بسبب الرقمنة السريعة للعمليات وتقديم الخدمات المالية، والوضع أسوأ من ذلك لأن تقدير الخسائر الاقتصادية الناجمة عن إختراق الأمن السيبراني أمر معقد للغاية بسبب التأثيرات متعددة الأبعاد للاختراق الأمني على المخاطر التشغيلية للبنوك والتكاليف والأداء (Lewis & Baker, 2013; Peng et al., 2017; Lever & Kifayat, 2020)، ويعني ذلك أن مخاطر الأمن السيبراني تؤدي إلى تصعيد المخاطر التشغيلية التي تؤدي بدورها إلى إرتفاع التكاليف التشغيلية للتأثير سلبًا على النتائج المالية للبنوك والمؤسسات المالية.(Kopp et al., 2017; Fitch, 2017; Aldasoro et al., 2020 a; Aldasoro et al., 2020 b)

ويتم إستخدام الكمبيوتر في الجرائم الإلكترونية إما كوسيلة لارتكاب جريمة أو كنظام تسجيل أو كهدف للجريمة (Padmaavathy, 2019)، فقد تقوم أجهزة الكمبيوتر إما بتخزين البيانات كجهاز تخزين يساعد على تنفيذ جريمة لا يجوز لأصحابها إمتلاكها مثل سرقة الملكية الفكرية، وقد ذكر (Njoroge, 2017) أنه من أجل حماية النظام المصرفي الإلكتروني من الهجمات السيبرانية، يجب الإنفاق في الأمن السيبراني للحد من مخاطره، وتتكون تكاليف الإنفاق في الأمن السيبراني من: (Njoroge, 2017)

١. تكلفة المنع (الوقاية) والكشف عن الجرائم السيبرانية (PDC) Prevention and Detection Costs.
٢. تكلفة تطوير الأمن السيبراني Development Costs (DC).

وسيتم تناول أنواع الإنفاق في الأمن السيبراني المتمثل في تكاليف المنع (الوقاية) والكشف عن الجرائم السيبرانية وتكلفة تطوير الأمن السيبراني في الجزء التالي.

٤-٢ أنواع الإنفاق في الأمن السيبراني:

يتكون الإنفاق في الأمن السيبراني من نوعين من التكاليف هما: تكاليف المنع والكشف عن الجرائم السيبرانية وتكاليف تطوير الأمن السيبراني، ويتم تناولهم على النحو التالي Khalil, (2020):

١. تكاليف المنع (الوقاية) والكشف عن الجرائم السيبرانية :

في أي بيئة محفوفة بالمخاطر عادة ما تتخذ أي مؤسسة وكذلك الأفراد تدابير لتقليل مقدار الخسارة التي قد يعانون منها نتيجة للوضع السيئ في حالة الجرائم الإلكترونية ذات الصلة (Lewis & Baker, 2013). ويشمل ذلك التدابير الأمنية الفردية والتنظيمية (مثل تثبيت الحماية المادية والافتراضية مثل البرامج المضادة للفيروسات)، وتكاليف التأمين والتكاليف المرتبطة بالإمتثال لمعايير تكنولوجيا المعلومات المطلوبة (مثل بطاقات الدفع، معيار أمان بيانات the Payment) Card Industry, Data Security Standard, PCI DSS) (Anderson et al, 2013)

وتعرف تكاليف الوقاية والكشف عن الجرائم السيبرانية بأنها "المعادل النقدي لأي جهود لتجنب الجرائم الإلكترونية" (Lewis & Baker, 2013)، وهي تشمل تكلفة تحديث أجهزة الكمبيوتر من خلال تطبيق نظام مكافحة الفيروسات، حيث لن يعمل نظام مكافحة الفيروسات إلا إذا تمت مراقبة نشر أجهزة الكمبيوتر من وقت لآخر، وتكلفة صيانة التدابير الوقاية، والنصائح التالية هي طرق أساسية يمكن من خلالها منع الجرائم الإلكترونية: حافظ على تحديث نظام الكمبيوتر، سيستخدم مجرمو الإنترنت عيوب البرامج لمهاجمة أنظمة الكمبيوتر بشكل متكرر ومجهول، يمكن تهيئة معظم الأنظمة المستندة إلى Windows لتنزيل تصحيحات البرامج وتحديثاتها تلقائيًا (Anderson et al, 2013)، وفي كثير من الأحيان يكون من الصعب تخصيصها لأنواع فردية من الجرائم الإلكترونية، ويمكن للدفاعات أن تستهدف الجرائم الفعلية أو البنية التحتية الداعمة لها، كما يمكن تكبد التكاليف تحسبا للجرائم أو رد فعل عليها، وقد تم التأكيد في العديد من الأبحاث والدراسات على أن المؤسسات غير الفاعلة في مكافحة الجرائم السيبرانية، سيمكن المحتالون عبر الإنترنت من الهجوم السيبراني عليهم وتعرض تلك المؤسسات لخسائر كبيرة (Anderson et al, 2013)، لذا يتعين على تلك المؤسسات دائمًا الإنفاق على الأمن السيبراني، ولكن إذا افترضنا أن نسبة معينة من الإنفاق الحالي لن تكون ضرورية في بيئة سيبرانية أكثر أمانًا، فإن هذا الإنفاق الإضافي يعتبر جزءًا من التكلفة الإجمالية (Lewis & Baker, 2013، وتشمل تكلفة المنع (الوقاية) والكشف عن الجرائم السيبرانية ما يلي:

- أقساط التأمين
- تكلفة أنظمة أمن تكنولوجيا المعلومات مثل مرشحات البريد العشوائي وجدران الحماية وبرامج مكافحة الفيروسات وملحقات المتصفح لحماية المستخدمين.
- تكلفة عمليات تقييم مراجعة أمن البيانات.

٢. تكلفة تطوير الأمن السيبراني:

وهي تكاليف تتعلق بالجودة وصيانة الأمن السيبراني وتشمل(Khalil, (2020 :

١. تكلفة تحليل وتقييم نظم أمن البيانات والمعلومات: ويتم فيها التركيز على البنية التحتية المناسبة لأمن البيانات وتشمل التكاليف التالية: https://2u.pw/X40G5U0

- تكلفة فحص الثغرات الأمنية: عادةً ما يتم الفحص التلقائي بواسطة فريق تكنولوجيا المعلومات، ويمكن إجراء الفحص الآلي للثغرات الأمنية أسبوعيًا أو شهريًا.
- تكلفة إختبار الاختراق (إختبار القلم): هو محاكاة لهجوم إلكتروني ويمكن إجراء إختبار القلم كل ثلاثة أشهر.
- تكلفة إختبار الفريق الأحمر: وهو إختبار أمان يتم على نطاق أوسع يتضمن المزيد من المشاركين ويتطلب المزيد من الموارد ويتم عمله نصف سنوي.

٢. تكلفة تطوير نظم أمن البيانات والمعلومات.

٣. تكلفة تدريب العاملين على أمن البيانات: ويتم فيها تزويد الموظفين بالمعرفة والمهارات الحديثة اللازمة لمنع انتهاكات البيانات أو تقليل تأثيرها، ويظل العامل البشري أحد أكبر مخاطر أي نظام لأمن البيانات. وفقًا لتقرير IBM Security ، ترتبط حوالي ٣٦ ٪ من خروقات البيانات الضارة بالسلوك البشري (التصيد الاحتيالي، والهندسة الاجتماعية، وبيانات الاعتماد المخترقة)، وأحد الحلول هو أتمتة عمليات معينة وتقليل دور المشغل البشري إلا في الحالات التي تكون الأتمتة غير ممكنة فيكون التعليم والتدريب هو الحل. https://bscdesigner.com/ar/cybersecurity-strategy.htm.

ولا شك أن الإنفاق في الأمن السيبراني يساهم في تخفيض مخاطر الأمن السيبراني الأمر الذي سيكون له تأثير إيجابي على الأداء المالي وغير المالي للبنوك التجارية، كما أن إنخفاض الإستثمار في الأمن السيبراني يساهم في زيادة المخاطر السيبرانية، والتي تؤدي بدورها إلى زيادة الخسائر المدفوعة عن المخاطر السيبرانية، لذا يلزم الأمر التعرض بإختصار للخسائر الناتجة عن حدوث المخاطر السيبرانية كما هو موضح في الجزء التالي.

٤-٣ الخسائر ناتجة عن المخاطر السيبرانية

وينتج عن المخاطر السيبرانية نوعين من الخسائر تتحملهم البنوك وهم:

١. خسائر الإستجابة للجرائم السيبرانية:

ويأخذ هذا في الإعتبار الخسائر المباشرة التي يتحملها الأفراد والشركات (بما في ذلك تكاليف إستمرارية الأعمال والإستجابة للتعافي من الكوارث)، وكذلك تشمل تكاليف دفع التعويضات لضحايا سرقة الهوية والغرامات التنظيمية من هيئات الصناعة والتكاليف غير المباشرة المرتبطة بالمسائل القانونية أو الطب الشرعي، وتشمل تكلفة الاستجابة للجرائم السيبرانية ما يلي (Anderson et al, 2013 Khalil, 2020):

- دفع التعويضات.
- الغرامات التنظيمية.
- التكاليف القانونية.

٢. الخسائر غير المباشرة:

وهي الخسائر غير المباشرة الناشئة عن إنخفاض الإستغلال التجاري للملكية الفكرية من خلال ضعف القدرة التنافسية، والتكاليف التبعية وهي تلك التي أثرت على البنك بشكل مباشر

(Anderson et al, 2013)، وتشمل هذه التكاليف الإجراءات ذات الصلة التي يتعين على البنك اتخاذها للرد على الخسائر التي قد تتكبدها أطراف أخرى مثل العملاء نتيجة لهجوم عبر المنصات عبر الإنترنت، وتشمل (Khalil, 2020 ; Lewis & Baker, 2013))

- الإضرار بالسمعة
- فقدان ثقة العملاء
- إنخفاض إستخدام المواطنين للخدمات الإلكترونية نتيجة لإنخفاض الثقة في المعاملات عبر الإنترنت
- الجهود المبذولة لتنظيف أجهزة الكمبيوتر المصابة بالبرامج الضارة لشبكة الروبوتات التي ترسل البريد العشوائي.

كما تعاني البنوك من إنخفاض قيمتها بعد الإبلاغ العلني عن تعرضها للاختراق، وعادة ما يكون ذلك في شكل إنخفاض في أسعار الأسهم (Lewis & Baker, 2013)، وسيتم التركيز على هدف البحث وهو الإنفاق في الأمن السيبراني.

٤-٤ حجم الإنفاق في الأمن السيبراني

هناك العديد من العوامل التي ينبغي مراعاتها عند تحديد حجم الإنفاق في الأمن السيبراني منها :https://2u.pw/5M3ZhTz

١. خرافة حماية جميع الأصول في البنك بنفس الطريقة

تعد بيانات العملاء المرتبطة ببرنامج بطاقة الائتمان الخاصة بالبنك أو برنامج بطاقة الولاء لمتاجر التجزئة ذات قيمة أكبر من أرقام الفواتير العامة ووثائق السياسة التي تنشئها الشركات داخل الشركة، ولا تمتلك البنوك موارد لا نهاية لها لحماية جميع البيانات بأي ثمن، فينبغي أن توفر إستراتيجية الأمن السيبراني القوية حماية مختلفة لأهم أصول الشركة، وذلك بإستخدام مجموعة متدرجة من التدابير الأمنية، كما يجب على قادة الأعمال والأمن السيبراني العمل معًا لتحديد وحماية "جواهر التاج" وهي تلك أصول الشركات التي تولد أكبر قيمة للبنك.

٢. خرافة كلما أنفقنا أكثر أصبحنا أكثر أمانًا

بعض البنوك التي تنفق قدرًا كبيرًا على الأمن السيبراني يكون أداؤها في الواقع أقل من أداء بقية السوق فيما يتعلق بتطوير المرونة الرقمية، ويرجع ذلك جزئيا إلى أن تلك البنوك لم تكن بالضرورة تحمي الأصول الصحيحة، كما ذكرنا سابقًا، غالبًا ما تلجأ البنوك إلى إتباع منهج شامل (حماية جميع الأصول بدلاً من حماية جواهر التاج).

٣. خرافة المتسللين الخارجيين هم التهديد الوحيد لأصول البنك

صحيح أن التهديدات من خارج البنك تشكل مصدر قلق كبير لفرق الأمن السيبراني، ولكن هناك تهديدات كبيرة من داخل البنك نفسه، وغالبًا ما يكون الأشخاص الأقرب إلى البيانات أو أصول البنك الأخرى بمثابة حلقة ضعيفة في برنامج الأمن السيبراني للبنك، خاصة عندما يشاركون كلمات المرور أو الملفات عبر شبكات غير محمية، أو ينقرون على الإرتباطات التشعبية الضارة المرسلة من عناوين بريد إلكتروني غير معروفة، أو يتصرفون بطرق أخرى تفتح شبكات البنك للهجوم، وفي الواقع تمثل التهديدات من داخل البنوك حوالي ٤٣% من خروقات البيانات .

https://2u.pw/5M3ZhTz، لذا يجب على قادة الأعمال والأمن السيبراني التعاون بشأن طرق تحسين ثقافة المخاطر الداخلية، والعمل على تثقيف الموظفين على جميع المستويات حول واقع التهديدات والهجمات السيبرانية وأفضل الممارسات لصدها.

٤. خرافة كلما كانت تقنيتنا أكثر تقدمًا كلما أصبحنا أكثر أمانًا

صحيح أن فرق الأمن السيبراني غالبًا ما تستخدم تقنيات قوية ومتطورة لحماية البيانات وأصول البنك، ولكن من الصحيح أيضًا أن العديد من التهديدات يمكن تخفيفها بإستخدام أساليب أقل تقدمًا، حيث أن معظم البنوك لا تتعامل مع قراصنة من الدرجة العسكرية، فوفقًا للأبحاث فإن أكثر من ٧٠ % من الهجمات الإلكترونية العالمية تأتي من مجرمي ذوي دوافع مالية يستخدمون أساليب بسيطة من الناحية التقنية، مثل رسائل البريد الإلكتروني التصيديةhttps://2u.pw/5M3ZhTz، فعندما تستثمر البنوك في التقنيات المتقدمة، ولكنها لا تفهم أفضل السبل لإستخدامها أو لا تتمكن من العثور على إداريين ذوي مهارات مناسبة لإدارتها، فإنها تنتهي في نهاية المطاف إلى خلق أوجه قصور كبيرة داخل فريق الأمن السيبراني، وبالتالي تعريض برنامج الأمن السيبراني بشكل عام للخطر.

٤-٥ كيف ندير حجم الإنفاق في الأمن السيبراني في البنوك التجارية؟

يلعب متخصصو التكنولوجيا دورًا في إعادة تثقيف كبار المسؤولين في البنوك حول أفضل الممارسات في الإنفاق على الأمن السيبراني، وعلى وجه التحديد توضيح السبب وراء كون المنهج المتدرج للأمن السيبراني أكثر فعالية من التغطية الشاملة للجميع، فلا يمكن للميزانية أن تنمو أو تتقلص إعتمادًا على ما إذا كان البنك قد تعرض مؤخرًا لاقتحام النظام، لذا يجب مراعاة ما يليhttps://2u.pw/5M3ZhTz:

- يجب إعتبار الإنفاق في الأمن السيبراني بمثابة إنفاق رأسمالي دائم.
- يجب تحديد أولويات المخصصات على أساس مراجعة كامل مجموعة المبادرات الجارية.
- يجب أن يعمل محترفو الأعمال والتكنولوجيا معًا لإدارة المقايضات المرتبطة بالأمن السيبراني.

وعند مناقشة المبادرات التي يجب الإنفاق فيها والمبادرات التي يجب إيقافها يمكن لمحترفي الأعمال والأمن السيبراني إستخدام نموذج تصنيف المخاطر مع الإشارة إلى أربعة مستويات للتهديد، من البسيط إلى الشديد. يمكن لفريق الأمن السيبراني إشراك المديرين التنفيذيين في المناقشات حول أصول البيانات الأكثر أهمية المرتبطة بكل جزء من سلسلة قيمة الأعمال، والأنظمة الموجودة فيها، والضوابط المطبقة، والمقايضات المرتبطة بحماية الأولوية العليا للأصول مقابل الأصول ذات الأولوية الأقل.

وعلى مستوى أوسع يمكن لمحترفي التكنولوجيا مساعدة كبار المسؤولين في إنشاء معايير للإنفاق في الأمن السيبراني في البنوك على مبادرات الأمن السيبراني التي يمكن مراجعتها بانتظام، على سبيل المثال الإنفاق على الأمن السيبراني كنسبة مئوية من إجمالي نفقات تكنولوجيا المعلومات، ويمكن أن يقوم مدير تكنولوجيا المعلومات وفريقه بإنشاء مؤشر للنفقات الرأسمالية للاستثمارات الأمنية لمساعدة المديرين التنفيذيين على تبرير التكلفة لكل خسائر معدلة حسب المخاطر أو التكلفة لكل نسبة مئوية من البنية التحتية المحمية أو يمكن لمحترفي التكنولوجيا والأعمال تطوير صيغة

مشتركة لقياس الإتجاه الصعودي لإجراء تحسينات على برنامج الأمن السيبراني، وبهذه الطريقة يمكنهم إتخاذ قرارات واضحة بشأن الأدوات التي يجب شراؤها وإضافتها إلى بنية الأمن السيبراني الحالية، والأنظمة التي يجب ترقيتها، والأنظمة التي سيتم إيقافها https://2u.pw/5M3ZhTz .

وبغض النظر عن المقاييس المستخدمة فمن المهم أن تكون هناك عملية تخطيط ومراجعة شاملة للإنفاق في الأمن السيبراني في البنوك، كما يجب تحديد الأولويات من منظور الأعمال بدلاً من منظور الأنظمة، وأن يتعاون مدراء تكنولوجيا المعلومات وكبار مسؤولي الأمن مع إدارة البنك لتحديد تلك الأصول التي لديها القدرة على توليد أكبر قدر من القيمة للبنك وتطوير خريطة طريق للأمن السيبراني وفقًا لذلك، مع ضرورة أن توضح خريطة الطريق توزيع جواهر التاج عبر البنك وأكبر مساحات التعرض للمخاطر السيبرانية، وبطبيعة الحال سيحتاج المسؤولون التنفيذيون في مجال الأعمال والأمن السيبراني في البنوك إلى إعادة النظر في هذه الخطط الربع سنوية أو السنوية للتأكد من أنها لا تزال ذات صلة بالنظر إلى التغييرات التي تطرأ على البيئة . https://2u.pw/5M3ZhTz

٤-٦ دور الإنفاق في الأمن السيبراني في تخفيض المخاطر السيبرانية

إن المؤسسات المالية بحاجة إلى الإنفاق في الأمن السيبراني بشكل كافٍ لتخفيض المخاطر السيبرانية من خلال بناء بنية تحتية تكنولوجية مرنة عبر الإنترنت على النحو الموصي به من قبل المنظمات الدولية (BIS, 2016)، فالإنفاق يحتاج في الغالب يتم في مجالات مثل إقتناء الأجهزة والبرامج الأكثر موثوقية، وأنظمة تشفير البيانات، وجدران الحماية، والمراقبة السيبرانية، وأنظمة الكشف عن المخاطر، والتدريب على تكنولوجيا المعلومات، وهناك تصور عام بأن الاتصال عبر الإنترنت محفوف بالمخاطر بطبيعته بسبب الجرائم السيبرانية وفشل النظام، لكن بعض الدراسات التجريبية وجدت أن إستخدام الإنترنت أكثر أمانًا الآن من ذي قبل نظرًا لأن الحوادث السيبرانية لكل وحدة من حركة البيانات عبر الإنترنت تقل مع الزيادة حجم حركة المرور (Kox, 2013; Paul & Wang, 2019; Ni et al., 2019)

ويشير تزايد الخروقات السيبرانية إلى ضعف أنظمة الشبكات، حيث يمكن أن يتسبب هجوم واحد في خسارة مالية وغير مالية كبيرة للبنك، على سبيل المثال أدت عملية اختراق واحدة لرمز SWIFT إلى سحب ٨١ مليون دولار أمريكي من حساب البنك المركزي في بنغلاديش لدى الاحتياطي الفيدرالي الأمريكي (Gopalakrishnan & Ogato, 2016)، وقد يمتد تأثير هذا الإختراق السيبراني إلى جميع المؤسسات المالية المشاركة في سلسلة المعالجة إذا لم يتم تأمين ثغرة النظام على مستوى البنك بشكل كافٍ، ولذلك تحتاج البنوك والمؤسسات المالية إلى توفير ميزانية كافية لشراء التكنولوجيا المناسبة للحفاظ على مرونة البنية التحتية السيبرانية في مواجهة التهديدات الأمنية (Johnson, 2015)، وقد أظهر إستطلاع أن المؤسسات المالية تأخذ التهديدات الأمنية على محمل الجد وتزيد إستثماراتها في البنية التحتية السيبرانية (PWC, 2015) نظرًا لأن المؤسسة المالية التي لا تمتلك بنية تحتية إلكترونية مرنة تكون معرضة بدرجة كبيرة للمخاطر السيبرانية (Germano, 2014).

وفقًا لتقرير الأمن السيبراني للصناعة المالية لعام ٢٠١٦، تعد الجرائم الإلكترونية المصدر الثاني للجرائم الإقتصادية في المؤسسات المالية العالمية (Security Scoreboard, 2016)، والعديد منها عبارة عن إنتهاكات واسعة النطاق وعمليات إحتيال وسرقات، حيث أن القطاع المالي

هو الهدف الرئيس لمجرمي الإنترنت (Ashford, 2019)، على سبيل المثال إستسلم البنك المركزي في بنجلاديش لقراصنة سويفت في عام ٢٠١٦ وخسر ٨١ مليون دولار أمريكي (Gladstone, 2016)، وقام قراصنة الإنترنت بتعطيل الشبكات المالية في كوريا الجنوبية لعدة أيام في عام ٢٠١٣ (Schwartz, 2013)، وبينما تقدم وكالات مختلفة أرقامًا مختلفة لخسائر البنوك على مستوى العالم يقدر صندوق النقد الدولي أن الخسائر السنوية قد تصل إلى حوالي ٩٧ مليارًا، وهو ما يمثل حوالي ٩% من صافي أرباح البنوك العالمية في عام ٢٠١٦ (Bouveret, 2018)، ولذلك تعمل البنوك والمؤسسات المالية على زيادة نفقاتها التكنولوجية بشكل مستمر للتغلب على التهديدات السيبرانية المتزايدة التي تزيد من تكاليف التشغيل (Euromoney, 2017)، ويظهر تقرير ديلويت أن نفقات التكنولوجيا للبنوك (كنسبة من إجمالي الإيرادات) ترتفع إلى ٧.١٦%، وهي الأعلى بين جميع قطاعات الاقتصاد العالمي (Kark et al., 2017). وهذا يشير إلى أن الصناعة المالية العالمية تتأثر سلبًا بالخسائر الناجمة عن إنتهاكات الأمن السيبراني.

وبشكل عام فإن مجموعة الأدبيات التي تم تطويرها تحمل بشكل عام إجماعًا على أن البنوك تتحمل عبئًا ماليًا إضافيًا ناتجًا عن الحوادث السيبرانية المتفشية التي تحدث بسبب الرقمنة السريعة للعمليات وتقديم الخدمات المالية، والوضع أسوأ من ذلك لأن تقدير الخسائر الاقتصادية الناجمة عن إختراق الأمن السيبراني أمر معقد للغاية بسبب التأثيرات متعددة الأبعاد للإختراق الأمني على المخاطر التشغيلية للبنوك والتكاليف والأداء، (Lewis & Baker, 2013; Peng et al., 2017; Lever & Kifayat, 2020) ، ويعني ذلك أن مخاطر الأمن السيبراني تؤدي إلى زيادة المخاطر التشغيلية التي تؤدي بدورها إلى ارتفاع التكاليف التشغيلية لتقليل الآثار الناتجة عن مخاطر الأمن السيبراني، بمعنى آخر أن زيادة الإنفاق في الأمن السيراني يقلل من مخاطر الأمن السيراني كمتغير وسيط، وإنخفاض مخاطر الأمن السيبراني يعمل على تحسين الأداء المالي في البنوك التجارية. (Kopp et al., 2017; Fitch, 2017; Aldasoro et al., 2020a; Aldasoro et al., 2020b).

٥. الإنفاق في الأمن السيبراني والأداء في البنوك التجارية في ظل توسيط المخاطر السيبرانية:

سيتم تتناول الإنفاق في الأمن السيبراني والمخاطر السيبرانية والأداء في البنوك التجارية على النحو التالي:

٥-١ أثر الإنفاق في الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية

تتمثل مخاطر الأمن السيبراني في المخاطر التكنولوجية والتشغيلية والتنظيمية التي تتعرض لها المنشآت المعتمدة على تقنيات تكنولوجيا المعلومات والناتجة عن اختراق نظام الأمن السيبراني لديها بما يحد من قدرته على تحقيق أهدافه (Badawy, 2021)، وتقسم هذه المخاطر إلى مجموعتين الأولى مخاطر الأداء التي تعبر عن فشل الأدوات التقنية في تحقيق أهدافها، والثانية المخاطر الأمنية وتشمل مخاطر الاختراق المادي، والتجسس بإستخدام أجهزة اختراق عن بعد، والمخاطر المرتبطة بسلوك العاملين، أما مخاطر المعلومات والإتصالات فتتضمن الهجمات على البيانات وهجمات البرامج الفيروسية، وتهدف الاختراقات الإلكترونية لإحداث اضطراب في العمليات التجارية والبنية التحتية لتحقيق مكاسب مالية للمخترق، أو إلحاق خسارة مالية، أو الإضرار بسمعة المنشأة المخترقة، أو تحقيق أهداف عسكرية، أو سياسية، أو نشر أيديولوجيات دينية (شحاتة، ٢٠٢٢). لذلك

يجب أن تحافظ البنوك على مستوى عال من الأمن السيبراني وتضع التدابير الوقائية لمواجهة الهجمات الإلكترونية المحتملة. ويركز الأمن السيبراني على كل إجراءات حماية البيانات، وتصميم وتطبيق برامج وآليات الدفاع الإلكتروني بما يحافظ على سالمة وأمن البيانات والأشخاص، ومن ثم استقرار البنوك من خلال القيام بالمراجعة لنظام الأمن السيبراني (Cheng et al, 2022)، لأن إنهيار هذا النظام قد يشير إلى ثغرة أمنية في البنية التحتية السيبرانية (Boin & McConnell, 2007; Brechbuhl et al., 2010; & Donge et al., 2018)، والتي تظهر كعامل خطر جديد في القطاع المالي (Kopp et al., 2017; Macaulay, 2018)، ولذلك فإن ثغرة النظام تخلق فرصة للمتسللين لإستغلال النظام وإلحاق خسائر مباشرة وغير مباشرة مما قد يؤثر على الأرباح في البنوك التجارية Juma'h & Alnsour, 2020; Kamiya et al., 2020; Skinner & (Sloan, 2002; BDO, 2017) والمخاطر (Srinidhi et al., 2015; OFR, 2017; Low, 2017; Peng et al., 2017) والنمو (Skinner & Sloan, 2002; BDO, 2017) من المؤسسات المنتهكة، وللحد من المخاطر السيبرانية يجب على البنوك تحقيق الأمن السيبراني من خلال الإنفاق في الأمن السيبراني والذي يترتب عليه نوعين من التكاليف هما: تكاليف المنع والكشف عن الجرائم السيبرانية وتكاليف تطوير الأمن السيبراني ، وتتكون تكاليف المنع والكشف عن الجرائم السيبرانية من أقساط التأمين، وتكاليف أنظمة أمان تكنولوجيا المعلومات مثل مرشحات البريد العشوائي وجدران الحماية وبرامج مكافحة الفيروسات وملحقات المتصفح لحماية المستخدمين، وتكاليف عمليات تقييم مراجعة أمن البيانات، أما تكلفة تطوير الأمن السيبراني فنشمل تكلفة تحليل وتقييم نظم أمن البيانات والمعلومات، تكلفة تطوير نظم أمن البيانات والمعلومات، وتكلفة تدريب العاملين على أمن البيانات، ولا شك أن الإنفاق على الامن السيبراني يترتب عليه تخفيض مخاطر الامن السيبراني، حيث أن زيادة الإنفاق في الأمن السيبراني سيؤدي إلى تخفيض المخاطر السيبرانية.

٥-٢ أثر تخفيض المخاطر السيبرانية على الأداء في البنوك التجارية:

يؤدي تخفيض المخاطر السيبرانية إلى تقليل الخسائر المترتبة على حدوث المخاطر السيبرانية في البنوك التجارية والتي تتمثل فيما يلي:

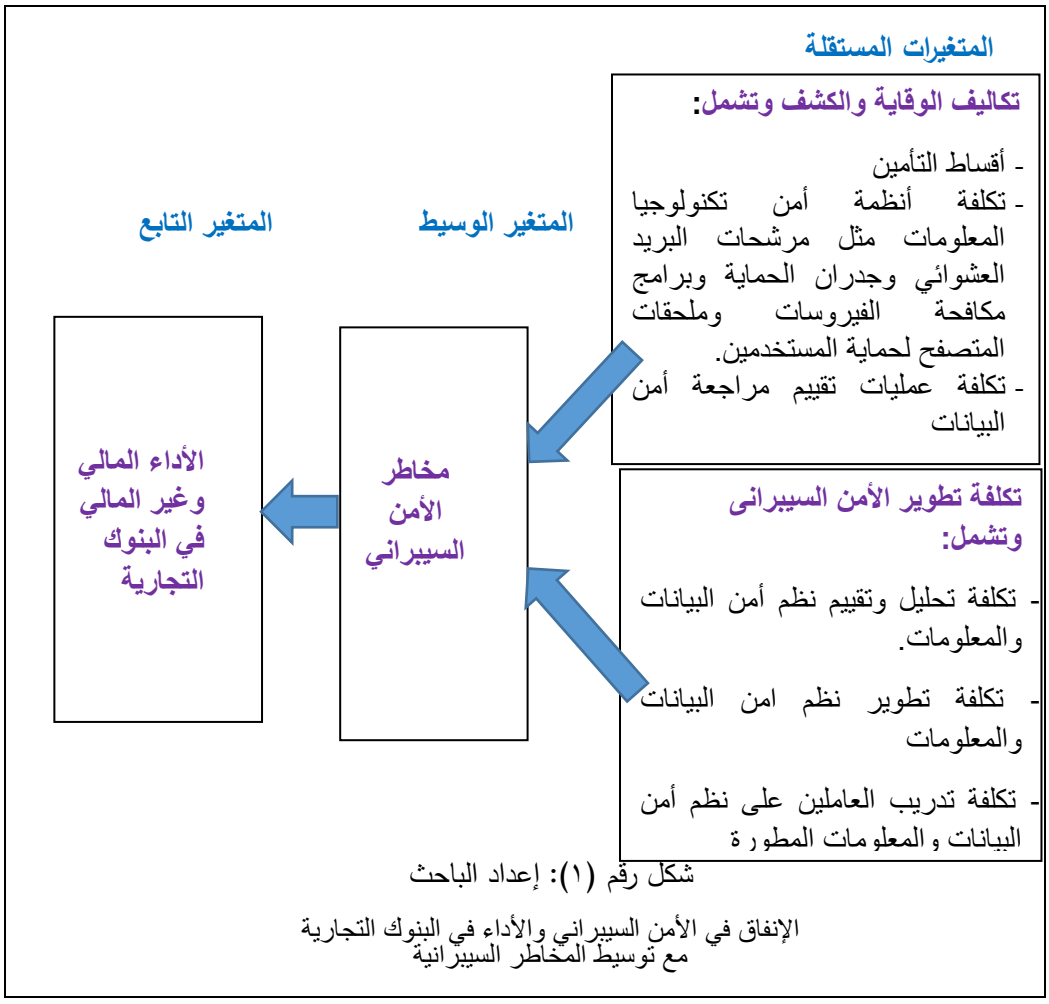
- خسائر الإستجابة للجرائم السيبرانية: والتي تشمل (دفع التعويضات، الغرامات التنظيمية، التكاليف القانونية (Anderson et al, 2013 Khalil, 2020).
- الخسائر غير المباشرة: والتي تشمل (الإضرار بالسمعة، فقدان ثقة العملاء، إنخفاض إستخدام المواطنين للخدمات الإلكترونية نتيجة لإنخفاض الثقة في المعاملات عبر الإنترنت، الجهود المبذولة لتنظيف أجهزة الكمبيوتر المصابة بالبرامج الضارة لشبكة الروبوتات التي ترسل البريد العشوائيKhalil, 2020 Lewis & Baker, 2013)).

ولا شك أن تخفيض خسائر الإستجابة للجرائم السيبرانية يؤدي إلى تحسين الأداء المالي للبنوك التجارية، أما تخفيض الخسائر غير المباشرة فيؤدي إلى تحسين الأداء غير المالي للبنوك التجارية، وحيث أن المعدل المتزايد بإستمرار لتغير التكنولوجيا يؤدي إلى زيادة أنشطة الجرائم الإلكترونية في القطاع المالي، وهذا في حد ذاته يدعو البنوك إلى زيادة الإنفاق في الأمن السيبراني بطرق متطورة للتخفيف من إحتمالات حدوث مخاطر الأمن السيبراني، ومن ثم تحسين أداء البنوك.

وللربط بين الإنفاق في الأمن السيبراني والأداء في البنوك التجارية في ظل توسيط المخاطر السيبرانية فسيتم في الجزء التالي عرض لمتغيرات البحث وهي الإنفاق في الامن السيبراني والمخاطر السيبرانية والأداء في البنوك التجارية والتي يسعى البحث لإختبار مدى صحتها أو عد صحتها.

٥-٣ متغيرات البحث

يهدف الباحث إلى تحديد ما إذا كانت المتغيرات المستقلة (تكلفة الوقاية والكشف، تكلفة تطوير الأمن السيبراني) لها تأثير على مخاطر الأمن السيبراني والأداء المالي وغير المالي في البنوك التجارية في ظل أخذ مخاطر الأمن السيبراني كمتغير وسيط بين الإنفاق في الأمن السيبراني والأداء في البنوك التجارية كما هو موضح في الشكل رقم (١) التالي:



شكل رقم (١): إعداد الباحث

الإنفاق في الأمن السيبراني والأداء في البنوك التجارية مع توسيط المخاطر السيبرانية

ويتضح من الشكل رقم (١) أن الإنفاق في الأمن السيبراني يتكون من: تكاليف المنع (الوقاية) والكشف عن الجرائم السيبرانية، وتكاليف تطوير الأمن السيبراني، وهذه التكاليف تمثل المتغيرات المستقلة والتي لها تأثير مباشر على المتغير التابع وهو مخاطر الأمن السيبراني، كما أن مخاطر

الأمن السيبراني يعد متغير وسيط يؤثر على الأداء المالي وغير المالي في البنوك التجارية، ويساهم الإنفاق في الأمن السيبراني في تقليل مخاطر الأمن السيبراني في البنوك التجارية والتي بدورها تساهم في تحسين الأداء المالي وغير المالي في البنوك التجارية وهو ما تسعى الدراسة الميدانية لإختبار مدى صحته.

ولأهمية العائد على الإستثمار الأمني في قرار الإنفاق في الأمن السيبراني فسوف يتم تناول دور العائد على الإستثمار الأمني في إتخار القرار الإستثماري في الجزء التالي.

٥-٤ دور العائد على الإستثمار الأمني في إتخار القرار الإستثماري Archie, Jackson, 2023; (https://2u.pw/1GGhOtD:([1])

يساعد تحليل العائد على الإستثمار الأمني في إتخار القرار الإستثماري ، ففي ظل توقع وصول تكاليف الجرائم السيبرانية للإقتصاد العالمي مبلغًا ضخمًا قدره ٦ تريليون دولار Archie (Jackson, 2023)، لذا تتطلع العديد من البنوك إلى زيادة استثماراتها في الأمن السيبراني، لكن زيادة الإستثمارات تتطلب تبريراً في شكل إيرادات، وتتمثل إستثمارات الأمن السيبراني في منتجات الأجهزة والبرامج المصممة لمنع الجرائم السيبرانية، وهذه النفقات تجعل من الصعب على فرق تكنولوجيا المعلومات والأمن تحديد العائدات على إستثماراتهم، ففي نهاية المطاف لن تستثمر أي قيادة عاقلة ملايين الدولارات في إستراتيجية ليس لها عوائد ملموسة، فغياب الأسباب الملموسة للإنفاق يسبب الإحباط بين محترفي تكنولوجيا المعلومات ويترك البنوك عرضة لثغرات أمنية سيبرانية صارخة وقراصنة خبيثين.

٥-٤-١ تحديد العائد على الإستثمار الأمني قبل الإستثمار في الحلول الأمنية:

كيف يمكنك تحديد قيمة شيء لا يحدث؟ تبدو الإجابة صعبة لكن ماذا لو قلنا لك أن هناك طريقة لتبرير هذه النفقات أو يطلق عليه العائد على الإستثمار الأمني Return on Security Investment (RoSI)، لذا من الضروري تحديد قيمة أو عائد الإستثمارات قبل الإستثمار في الحلول الأمنية للأسباب التالية:https://2u.pw/1GGhOtD; https://cutt.us/cIxSj:

١. يساعد تحديد قيمة الإستثمار أو عائده على ضمان توافق الإستثمار مع الأهداف الإستراتيجية للبنك.

٢. يساعد في تحديد أولويات الإستثمارات الأمنية بناءً على تأثيرها المحتمل على الوضع الأمني للبنك.

٣. يساعد على تبرير الإستثمار لأصحاب المصلحة وإظهار الفوائد الملموسة للإستثمار.

صحيح أن قياس قيمة أو عائد الإستثمار في الحلول الأمنية قد يكون أمرًا صعبًا لأن المخاطر والحوادث الأمنية غالبًا ما يكون من الصعب تحديدها كميًا، لكن يُعد (RoSI) أحد هذه المقاييس المستخدمة لقياس فعالية وقيمة الإستثمارات التي تتم في المبادرات الأمنية، ويتم حساب RoSI من خلال مقارنة تكلفة الإستثمارات الأمنية، مثل التكنولوجيا والموظفين والتدريب، بالفوائد المكتسبة من

[1] لمزيد من التفاصيل عن هذا الموضوع يمكن الرجوع إلى: (Archie, Jackson, 2023; https://2u.pw/1GGhOtD ; https://2u.pw/5M3ZhTz)

تلك الإستثمارات، مثل تقليل الخسائر، وعدد أقل من الحوادث الأمنية، وزيادة حماية الأصول القيمة، وROSI هو نسخة معدلة من حساب عائد الإستثمار، مع بعض التغييرات لإستيعاب تفرد الإستثمارات المتعلقة بالأمن السيبراني، فهو يقارن صافي فائدة إجمالي نفقات الخروقات الأمنية التي تم تجنبها مع تكلفة الوقاية المتكبدة، وهو يوفر صورة دقيقة عن مدى ربحية الإستثمار في الأمن السيبراني.

العائد على الإستثمار الأمني = (فوائد الإستثمار الأمني - تكلفة الإستثمار الأمني) / تكلفة الإستثمار الأمني

والعائد على الإستثمار الأمنيRoSI هو نسبة الفوائد النقدية للاستثمار الأمني إلى تكلفته، ويشير مؤشر RoSI الإيجابي إلى أن الإستثمار قد حقق عائدًا إيجابيًا صافيًا، بينما يشير مؤشر RoSI السلبي إلى أن الإستثمار أدى إلى خسارة صافية، ويمكن لـ RoSI مساعدة البنوك في تحديد الإستثمارات الأمنية التي تستحق الإنفاق وأيها لا تستحق ذلك من خلال تحليل فوائد وتكاليف المبادرات الأمنية المختلفة، كما يمكن للبنوك تخصيص مواردها الأمنية بشكل أكثر فعالية وكفاءة، ويتضمن تحليل RoSI تقييم تكاليف وفوائد المبادرات الأمنية وحساب مقياس RoSI لتحديد ما إذا كان الإستثمار قد حقق عائدًا إيجابيًا صافيًا.

٥-٤-٢ تحليل العائد على الإستثمار الأمني (RoSI):

قد تشمل الإستثمارات الأمنية التي يتم تقييمها الإستثمارات في التكنولوجيا أو الموظفين أو التدريب أو الموارد الأخرى المتعلقة بالأمن وتتضمن ما يليhttps://cutt.us/cIxSj:

١. تحديد تكاليف الإستثمارات: ويتضمن ذلك تحديد النفقات المرتبطة بكل استثمار، مثل تكلفة شراء وتنفيذ التكنولوجيا، ورواتب ومزايا أفراد الأمن، وتكلفة البرامج التدريبية.

٢. تحديد فوائد الإستثمارات: يتضمن ذلك تحديد تأثير الإستثمارات الأمنية على المنظمة، مثل تقليل المخاطر وزيادة حماية الأصول القيمة وتقليل عدد الحوادث الأمنية.

٣. حساب مقياس RoSI: بإستخدام الصيغة (فوائد الإستثمار الأمني - تكلفة الإستثمار الأمني) / تكلفة الإستثمار الأمني، يمكن حساب مقياس RoSI لتحديد العائد المالي على الإستثمار الأمني.

٤. تفسير النتائج: يشير مؤشر RoSI الإيجابي إلى أن الإستثمار قد حقق عائدًا إيجابيًا صافيًا، بينما يشير مؤشر RoSI السلبي إلى أن الإستثمار أدى إلى خسارة صافية، واستنادًا إلى نتائج التحليل يمكن للبنك اتخاذ قرارات حول كيفية تخصيص موارده الأمنية بشكل أكثر فعالية وكفاءة.

وفي أحد الدراسات https://cutt.us/cIxSj كان مؤشر RoSI يساوي ٥.٢٥ وهذا يعني أنه مقابل كل دولار يتم إنفاقه في الامن السيبراني يتوقع الحصول على فوائد مالية قدرها ٥.٢٥ دولار، وكما تشير قيمة RoSI الأقل من ١ إلى أن الفوائد المالية المتوقعة من الإستثمار الأمني قد لا تتجاوز تكاليفه، وبالتالي قد لا يكون الإستثمار هو الإستخدام الأكثر فعالية لميزانية الأمان الخاصة بالبنك، ومع ذلك هذا لا يعني بالضرورة أنه لا ينبغي القيام بالإستثمار، فقد تكون هناك فوائد غير مالية أخرى للاستثمار في الحلول الأمنية، مثل تحسين الوضع الأمني، وزيادة ثقة العملاء، وتحسين سمعة

العلامة التجارية، بالإضافة إلى ذلك يعد تحليل RoSI أداة واحدة فقط يمكن إستخدامها لتقييم الإستثمارات الأمنية، ويجب أيضًا مراعاة عوامل أخرى مثل إدارة المخاطر والامتثال التنظيمي Regulatory Compliance والأهداف الإستراتيجية، ومع ذلك في النهاية يجب أن يعتمد القرار بشأن الإستثمار في حل أمني أم لا على تقييم شامل لاحتياجات وأولويات البنك الأمنية.

٥-٤-٣ المعايير التي يجب مراعاتها لاتخاذ قرار أفضل عندما تكون قيمة RoSI أقل من ١:

عندما تكون قيمة RoSI أقل من (١) يجب مراعات المعايير التالية https://cutt.us/cIxSj:

١. إدارة المخاطر: يجب تقييم القرار الإستثماري بناءً على مستوى المخاطر التي يواجهها البنك، فإذا كان الحل الأمني ضروريًا للتخفيف من التهديدات عالية المخاطر، فقد يكون من الضروري الإستثمار حتى لو كان مؤشر RoSI أقل من ١.

٢. الإمتثال التنظيمي: قد يتطلب الإمتثال للوائح ومعايير الصناعة حلولاً أمنية محددة، والتي قد يكون لها مؤشر RoSI أقل ١، في هذه الحالة قد يكون الإستثمار ضروريًا للإمتثال للوائح وتجنب الغرامات.

٣. الأهداف الإستراتيجية: يجب أن يتوافق قرار الإستثمار مع الأهداف الإستراتيجية للمنظمة، على سبيل المثال إذا كانت المنظمة تخطط لتوسيع أعمالها في سوق جديد، فقد يكون من الضروري الإستثمار في الحلول الأمنية لكسب ثقة العملاء في ذلك السوق.

٤. الفوائد غير المالية: قد تكون هناك فوائد غير مالية للإستثمار في الحلول الأمنية، مثل تحسين سمعة العلامة التجارية وثقة العملاء ورضا الموظفين، وينبغي تقييم هذه الفوائد جنبا إلى جنب مع RoSI لاتخاذ القرار المناسب.

٥. الخيارات البديلة: يجب على البنك النظر في خيارات بديلة لمعالجة المخاطر الأمنية، على سبيل المثال قد يكون من الممكن الإستثمار في حل أمني مختلف يحتوي على RoSI أعلى أو إعادة تخصيص ميزانية الأمان لمعالجة المخاطر الأخرى.

٥-٤-٤ أدوات وأساليب تحليل الأخرى لتحديد العائد على الإستثمارات الأمنية.

هناك العديد من أدوات وأساليب التحليل الأخرى التي يمكن إستخدامها لتحديد العائد على الإستثمارات الأمنية تتمثل فيما يلي[٢] https://cutt.us/cIxSj:

١. التكلفة الإجمالية للملكية Total Cost of Ownership (TCO).

٢. تقييم المخاطر Risk Assessment>

٣. تحليل تأثير الأعمال Business Impact Analysis (BIA).

٤. تحليل التكلفة والعائد Cost-Benefit Analysis (CBA).

٥. تكلفة الاختراق Cost of a Breach (COB).

[٢] لمزيد من التفاصيل يمكن الرجوع إلى: https://cutt.us/cIxSj

٦. القيمة الاقتصادية المضافة Economic Value Added (EVA.

٧. قيمة تقليل المخاطر Risk Reduction Value (RRV.

٨. بطاقة الأداء المتوازنalanced Scorecard .

ويرى الباحث أنه لا توجد طريقة تحليل هي الأفضل على الإطلاق لحساب العائد على الإستثمار الأمني وتحديده، وإنما كل طريقة مزايا ونقاط ضعف الخاصة بها، وقد يكون من الضروري الجمع بين أساليب التحليل المتعددة للحصول على فهم شامل للعائد المحتمل على الإستثمار في الحلول الأمنية.

٥-٥ خلاصة الدراسة النظرية

خلصت الدراسة النظرية إلى أن زيادة الإنفاق في الأمن السيبراني المتمثل في منتجات الأجهزة والبرامج المصممة لمنع الجرائم السيبرانية والمضادة للفيروسات والتصيد الاحتيالي، أو إصابات البرامج الضارة، أو الوصول غير المصرح به إلى حسابات البريد الإلكتروني، بالإضافة إلى التدابير الأمنية في التخفيف من تلك المخاطر (تكلفة شراء وتنفيذ تكنولوجيا الامن السيبراني)، وتكاليف التأمين والتكاليف المرتبطة بالإمتثال لمعايير تكنولوجيا المعلومات المطلوبة لبرامج الحماية ضد الإختراق تؤدي إلى تخفيض المخاطر السيبرانية والتي من بينها الاختراقات السيبرانية، الاحتيال الإلكتروني، البرمجيات الخبيثة، الاختراقات الداخلية، النقص في الأمان والحماية، ومن جهة أخرى خلصت الدراسة إلى أن تخفيض المخاطر السيبرانية يؤدي إلى تحسين الأداء في البنوك التجارية سواء الأداء المالي أو الأداء غير المالي.

وفي القسم التالي يتم إختبار الدراسة ميدانياً على البنوك التجارية المصرية.

٦. الدراسة الميدانية

تستهدف الدراسة الميدانية إختبار فروض البحث الرئيسة وهي:

- مدى تأثير الإنفاق الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية.
- مدى تأثير المخاطر السيبرانية على الأداء المالي وغير المالي في البنوك التجارية.

وقد تم إختبار هذه الفروض الرئيسة من خلال إختبار مجموعة من الفروض الفرعية والتي يمثل كل منها أحد متغيرات البحث والتوصل إلى أدلة ميدانية تؤيد تلك الفروض أو لا تؤيدها في البنوك التجارية المصرية.

٦-١ الأساليب الإحصائية:

تم إستخدام الأساليب الإحصائية التالية في هذا البحث: إختبار كروسكال واليس

١. القياس الإحصائي الوصفي القائم على الحزم الإحصائية (SPSS) لوصف خصائص عينة البحث والحصول على المتوسطات الحسابية، والإنحرافات المعيارية، وتم الإعتماد على الوسط الحسابي الفرضي البالغ (٣) كمعيار لقياس وتقييم الدرجة المتحصل عليها من المستجوبين.
٢. إختبار كولمجروف – سمرنوف "Kolmogorov Smirnov "

٣. إختبار كروسكال – والاس "Kruskal-Wallis Test" لإختبار جوهرية الإختلافات بين متوسطات فئات المبحوثين.
٤. إختبار T لعينة واحدة لمقارنة المتوسطات المحسوبة مع متوسط القيم الجدولية المطبقة في هذا البحث لإختبار مدى تأثير الإنفاق في الأمن السيبراني على المخاطر السيبرانية والأداء في البنوك التجارية.

٦-٢ فروض الإحصائية للبحث:
١. لا يوجد أثر ذو دلالة إحصائية لتكلفة المنع والكشف عن الجرائم السيبرانية على المخاطر السيبرانية في البنوك التجارية المصرية.
٢. لا يوجد أثر ذو دلالة إحصائية لتكلفة تطوير الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية المصرية.
٣. لا يوجد أثر ذو دلالة إحصائية للإنفاق في الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية المصرية.
٤. لا يوجد أثر ذو دلالة إحصائية للمخاطر السيبرانية على الأداء المالي في البنوك التجارية المصرية.
٥. لا يوجد أثر ذو دلالة إحصائية للمخاطر السيبرانية على الأداء غير المالي في البنوك التجارية المصرية.
٦. لا يوجد أثر ذو دلالة إحصائية للمخاطر السيبرانية على الأداء المالي وغير المالي في البنوك التجارية المصرية.
٧. لا توجد إختلافات جوهرية بين آراء المبحوثين حول تأثير الإنفاق في الأمن السيبراني على المخاطر السيبرانية والأداء المالي وغير المالي في البنوك التجارية.

٦-٣ مجتمع وعينة الدراسة:

يتمثل مجتمع الدراسة الميدانية من مديري ونواب مديري الفروع ومدراء الأقسام والمصرفيين العاملين بالبنوك التجارية المصرية لتوافر وتنوع الخبرات والوعي لديهم، وتم تحديد عينة عشوائية عددها (٢٢٠) مفردة من مجتمع الدراسة، وتم تجميع عدد (١٨٠) استبانة صحيحة بنسبة (٨٢%) من إجمالي الإستبانات وهي نسبة جيدة لإجراء التحليل الاحصائي، ويعرض جدول رقم (٢) توزيع إستمارات الإستقصاء المستلمة من عينة الدراسة حسب فئات العينة والتي كانت على النحو التالي:

جدول رقم (٢)

توزيع إستمارات الإستقصاء المستلمة من عينة الدراسة حسب فئات العينة

المتغير	البيان	العدد	النسبة المئوية
المؤهل العلمي	بكالوريوس	١٤٠	%٧٧.٨
	ماجستير	٣٤	%١٨.٩
	دكتوراه	٦	%٣.٣
	المجموع	١٨٠	%١٠٠

المتغير	البيان	العدد	النسبة المئوية
المسمى الوظيفي	مدير فرع	٣٤	%١٨.٩
	نائب مدير فرع	٤٠	%٢٢.٢
	رئيس قسم	٤٤	%٢٤.٤
	مصرفي	٦٢	%٣٤.٥
	المجموع	١٨٠	%١٠٠
سنوات الخبرة	من ٥ – ١٠ سنوات	٦٦	%٣٦.٧
	١٠- ١٥ سنة	٥٤	%٣٠
	١٥- ٢٠سنة	٣٤	%١٨.٩
	أكبر من ٢٠ سنة	٢٦	%١٤.٤
	المجموع	١٨٠	%١٠٠

٦-٤ أداة البحث:

تم الاعتماد في تجميع البيانات على إستمارة استقصاء روعي في إعدادها البساطة والوضوح وسهولة الفهم، وتم تحكيمها من قبل مجموعة من المحكمين المتخصصين في المحاسبة في الجامعات حتى خرجت في صورتها النهائية، وقد تم إستخدام مقياس ليكرت الخماسي، وقد تم تقسيمها إلى جزئين كما يلي:

- الجزء الأول: ويتكون من البيانات الديمغرافية لعينة البحث ويتكون من ثلاث فقرات.
- الجزء الثاني: ويتناول أثر الإنفاق في الأمن السيبراني على المخاطر السيبرانية والأداء المالي وغير المالي في البنوك التجارية المصرية.

وكانت المصداقية على الاستبيان تبعا ألفا كرونباخ (٠.٨٨) وهي نسبة ممتازة كونها أعلى من النسبة المقبولة (٦٠%)، وهذا يعني توافر درجة كبيرة من المصداقية في إجابات الأسئلة.

٦-٥ قياس مدى تأثير الإنفاق في الأمن السيبراني على المخاطر السيبرانية والأداء المالي وغير المالي في البنوك التجارية المصرية.

تم قياس مدى تأثير الإنفاق في الأمن السيبراني على المخاطر السيبرانية والأداء المالي وغير المالي في البنوك التجارية المصرية من خلال إستبيان يتضمن مجموعة من العبارات التي تقيس ذلك، وقد تم إستخدام مقياس Likert ذو الخمس نقاط لتحديد أوزان العبارات وللتأكد من صحة فروض البحث من خلال الإجابة على السؤال الرئيس للبحث وهو:

- ما مدى تأثير الإنفاق في الأمن السيبراني على المخاطر السيبرانية والأداء المالي وغير المالي في البنوك التجارية المصرية؟

وقد تم إختبار مدى تأثير الإنفاق في الأمن السيبراني على المخاطر السيبرانية والأداء المالي وغير المالي في البنوك التجارية المصرية، حيث تم حساب المتوسط والإنحراف المعياري والوزن

النسبي لإجابات المستجوبين حول الأسئلة المطروح من الباحث حيث تم حساب المتوسط العام للإجابات المتعلقة بكل متغير من متغيرات البحث، ثم حساب متوسط الوزن لجميع المتوسطات وكذلك إختبار T لعينة واحدة One Sample T- Test (الجداول من رقم ٣-١١).

٦-٦ إختبار فروض الدراسة الميدانية:

تم إختبار الفروض الإحصائية للدراسة الميدانية على النحو التالي:

١. الفرض الأول: لا يوجد أثر ذو دلالة إحصائية لتكلفة المنع والكشف عن الجرائم السيبرانية على المخاطر السيبرانية في البنوك التجارية المصرية.

يبين الجدول رقم (٣) نتائج مدى تأثير تكلفة المنع والكشف عن الجرائم السيبرانية على المخاطر السيبرانية في البنوك التجارية المصرية من خلال الوسط الحسابي والإنحراف المعياري وإختبارT لعينة واحدة وإختبار كولمجروف - سمرنوف والأهمية النسبية.

جدول رقم (٣)

نتائج مدى تأثير تكلفة المنع والكشف عن الجرائم السيبرانية على المخاطر السيبرانية في البنوك التجارية المصرية

البيان	الوسط الحسابي	الانحراف المعياري	الأهمية النسبية	قيمة (T) المحسوبة	كولمجروف - سمرنوف	مستوى المعنوية
١. تساهم تكاليف أنظمة أمن تكنولوجيا المعلومات مثل مرشحات البريد العشوائي وجدران الحماية وبرامج مكافحة الفيروسات وملحقات المتصفح لحماية المستخدمين في تخفيض المخاطر السيبرانية في البنوك التجارية.	٤.٧٥	٠.١١	٠.٩٧	٢١.٣٢	٠.٩٤	٠.٠٠
٢. تساهم تكاليف التأمين للأمن السيبراني في تخفيض المخاطر السيبرانية في البنوك التجارية.	٤.٣٢	٠.١٥	٠.٩١	٢١.٣٢	٠.٩٤	٠.٠٠
٣. تساهم التكاليف المرتبطة بالامتثال لمعايير تكنولوجيا المعلومات المطلوبة في تخفيض المخاطر السيبرانية في البنوك التجارية.	٤.٥٥	٠١٣	٠.٩٤	٢١.٣٢	٠.٩٤	٠.٠٠
٤. تساهم التكاليف الصيانة والتدابير الوقائية للأمن السيبراني في تخفيض المخاطر السيبرانية في البنوك التجارية.	٤.٦٧	٠.١٢	٠.٩٥	٢١.٣٢	٠.٩٤	٠.٠٠
المتوسط	٤.٥٧	٠.١٣	٠.٩٤	٢١.٣٢	٠.٩٤	٠.٠٠

تبين من الجدول رقم (٣) أن قيمة الوسط الحسابي مدى تأثير تكلفة المنع والكشف عن الجرائم السيبرانية على المخاطر السيبرانية في البنوك التجارية المصرية بلغت (٤.٥٧) وبالمقارنة بالوسط الحسابي الفرضي البالغ (٣) كمعيار لقياس وتقييم الدرجة المتحصل عليها، وكذلك نتائج إختبار Tعينة واحدة ونتائج إختبار كولمجروف - سمرنوف والتي تشير لعدم وجود إختلافات جوهرية بين مفردات العينة، تم رفض فرض العدم وقبول الفرض البديل وهو: يوجد أثر ذو دلالة إحصائية لتكلفة المنع والكشف عن الجرائم السيبرانية على المخاطر السيبرانية في البنوك التجارية المصرية.

٢. الفرض الثاني: لا يوجد أثر ذو دلالة إحصائية لتكاليف تطوير الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية المصرية.

يبين الجدول رقم (٤) نتائج مدى تأثير تكاليف تطوير الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية المصرية، من خلال الوسط الحسابي والإنحراف المعياري وإختبار Tلعينة واحدة والأهمية النسبية.

جدول رقم (٤)

نتائج مدى تأثير تكاليف تطوير الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية المصرية.

البيان	الوسط الحسابي	الانحراف المعياري	الأهمية النسبية	قيمة ( ) T المحسوبة	كولمجروف - سمرنوف	مستوى المعنوية
١. تساهم تكاليف فحص الثغرات الأمنية في تخفيض المخاطر السيبرانية في البنوك التجارية	٤.٦٤	٠.١٠	٠.٩٤	٢١.٣٢	٠.٩٤	٠.٠٠
٢. تساهم تكاليف إختبار الاختراق في تخفيض المخاطر السيبرانية في البنوك التجارية	٤.٥١	٠.١٦	٠.٨٩	٢١.٣٢	٠.٩٤	٠.٠٠
٣. تساهم تكاليف عمليات مراجعة أمن البيانات في تخفيض المخاطر السيبرانية في البنوك التجارية.	٤.٤٦	٠.١٤	٠.٨٨	٢١.٣٢	٠.٩٤	٠.٠٠
٤. تساهم تكاليف تزويد الموظفين بالمعرفة والمهارات الحديثة اللازمة لمنع انتهاكات البيانات في تخفيض المخاطر السيبرانية في البنوك التجارية	٤.٥٢	٠.١٢	٠.٩٠	٢١.٣٢	٠.٩٤	٠.٠٠
المتوسط	٤.٥٣	٠.١٣	٠.٩٠	٢١.٣٢	٠.٩٤	٠.٠٠

تبين من الجدول رقم (٤) أن قيمة الوسط الحسابي لمدى نتائج مدى تأثير تكاليف تطوير الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية المصرية بلغت (٤.٥٤) وبالمقارنة بالوسط الحسابي الفرضي البالغ (٣) كمعيار لقياس وتقييم الدرجة المتحصل عليها، وكذلك نتائج إختبار T لعينة واحدة ونتائج إختبار كولمجروف - سمرنوف والتي تشير لعدم وجود إختلافات جوهرية بين

مفردات العينة، تم رفض فرض العدم وقبول الفرض البديل وهو: يوجد أثر ذو دلالة إحصائية لتكاليف تطوير الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية المصرية.

٣. الفرض الثالث: لا يوجد أثر ذو دلالة إحصائية للإنفاق في الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية.

يبين لنا من نتائج الجدولين رقم (٣) ورقم (٤) نتائج مدى تأثير الإنفاق في الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية، من خلال الوسط الحسابي والإنحراف المعياري وإختبار Tلعينة واحدة والأهمية النسبية.

جدول رقم (٥)

نتائج مدى تأثير الإنفاق في الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية المصرية

البيان	الوسط الحسابي	الانحراف المعياري	الأهمية النسبية	قيمة (T) المحسوبة	كولمجروف - سمرنوف	مستوى المعنوية
متوسط نتائج مدى تأثير تكلفة المنع والكشف عن الجرائم السيبرانية على المخاطر السيبرانية في البنوك التجارية المصرية	٤.٥٧	٠.١٣	٠.٩٤	٢١.٣٢	٠.٩٤	٠.٠٠
متوسط نتائج مدى تأثير تكاليف تطوير الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية المصرية.	٤.٥٤	٠.١٣	٠.٩٠	٢١.٣٢	٠.٩٤	٠.٠٠
المتوسط	٤.٥٥	٠.١٣	٠.٩٢	٢١.٣٢	٠.٩٤	٠.٠٠

تبين من الجدول رقم (٥) أن قيمة الوسط الحسابي لمدى مدى تأثير الإنفاق في الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية بلغت (٤.٥٥) وبالمقارنة بالوسط الحسابي الفرضي البالغ (٣) كمعيار لقياس وتقييم الدرجة المتحصل عليها، وكذلك نتائج إختبار T لعينة واحدة ونتائج إختبار كولمجروف - سمرنوف والتي تشير لعدم وجود إختلافات جوهرية بين مفردات العينة، تم رفض فرض العدم وقبول الفرض البديل وهو: يوجد أثر ذو دلالة إحصائية للإنفاق في الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية المصرية.

٤. الفرض الرابع: لا يوجد أثر ذو دلالة إحصائية المخاطر السيبرانية على الأداء المالي في البنوك التجارية المصرية.

يبين الجدول رقم (٦) نتائج مدى تأثير المخاطر السيبرانية على الأداء المالي في البنوك التجارية المصرية من خلال الوسط الحسابي والإنحراف المعياري وإختبار T لعينة واحدة والأهمية النسبية.

جدول رقم (٦)

نتائج مدى تأثير المخاطر السيبرانية على الأداء المالي في البنوك التجارية المصرية

البيان	الوسط الحسابي	الانحراف المعياري	الأهمية النسبية	قيمة (T) المحسوبة	كولمجروف - سمرنوف	مستوى المعنوية
١. يساهم تخفيض مخاطر الأمن السيبراني في زيادة قيمة السوقية لأسهم البنك	٤.٦٢	٠.١٠	٠.٩٣	٢١.٣٢	٠.٩٤	٠.٠٠
٢. يساهم تخفيض مخاطر الأمن السيبراني في تخفيض قيمة التعويضات المدفوعة	٤.٣٨	٠.١٧	٠.٩٠	٢١.٣٢	٠.٩٤	٠.٠٠
٣. يساهم تخفيض مخاطر الأمن السيبراني في تخفيض قيمة الغرامات التنظيمية	٤.٤٣	٠.١٥	٠.٨٩	٢١.٣٢	٠.٩٤	٠.٠٠
٤. يساهم تخفيض مخاطر الأمن السيبراني في تخفيض التكاليف القانونية	٤.٥١	٠.١١	٠.٩٢	٢١.٣٢	٠.٩٤	٠.٠٠
٥. يساهم تخفيض مخاطر الأمن السيبراني في تخفيض تكاليف الاستجابة للتعافي من الكوارث.	٤.٥٣	٠.١١	٠.٩	٢١.٣٢	٠.٩٤	٠.٠٠
٦. يساهم تخفيض مخاطر الأمن السيبراني في تخفيض تكاليف استمرارية الأعمال.	٤.٣١	٠.١٦	٠.٨٤	٢١.٣٢	٠.٩٤	٠.٠٠
٧. يساهم تخفيض مخاطر الأمن السيبراني في زيادة ربحية البنك.	٤.٦٨	٠.٠٩	٠.٨٩	٢١.٣٢	٠.٩٤	٠.٠٠
٨. يساهم تخفيض مخاطر الأمن السيبراني في زيادة معدل العائد على الإستثمار في البنك.	٤.٧٢	٠.٠٨	٠.٩٥	٢١.٣٢	٠.٩٤	٠.٠٠
٩. يساهم تخفيض مخاطر الأمن السيبراني في زيادة معدل العائد على حقوق الملكية في البنك	٧.٧٦	٠.٠٧	٠.٩٦	٢١.٣٢	٠.٩٤	٠.٠٠
المتوسط	٤.٨٨	٠.١١	٠.٩١	٢١.٣٢	٠.٩٤	٠.٠٠

تبين من الجدول رقم (٦) أن قيمة الوسط الحسابي لمدى تأثير المخاطر السيبرانية على الأداء المالي في البنوك التجارية المصرية بلغت (٤.٨٨) وبالمقارنة بالوسط الحسابي الفرضي البالغ (٣) كمعيار لقياس وتقييم الدرجة المتحصل عليها، وكذلك نتائج إختبار T لعينة واحدة ونتائج إختبار كولمجروف - سمرنوف والتي تشير لعدم وجود إختلافات جوهرية بين مفردات العينة، تم رفض

فرض العدم وقبول الفرض البديل وهو: يوجد أثر ذو دلالة إحصائية للمخاطر السيبرانية على الأداء المالي في البنوك التجارية المصرية.

٥. الفرض الخامس: لا يوجد أثر ذو دلالة إحصائية المخاطر السيبرانية على الأداء غير المالي في البنوك التجارية المصرية.

ولقياس مدى تأثير المخاطر السيبرانية على الأداء غير المالي في البنوك التجارية المصرية، تم حساب المتوسط الحسابي العام والانحراف المعياري والأهمية النسبية وإختبار T لعينة واحدة للعينة محل الدراسة والتطبيق وكانت النتائج كما هي موضحة في الجدول رقم (٧).

جدول رقم (٧)

نتائج مدى تأثير المخاطر السيبرانية على الأداء غير المالي في البنوك التجارية المصرية

البيان	الوسط الحسابي	الانحراف المعياري	الأهمية النسبية	قيمة (T) المحسوبة	كولمجروف ـ سمرنوف	مستوى المعنوية
١. يساهم تخفيض مخاطر الأمن السيبراني في تعزيز رضا العملاء	٤.٦١	٠.١٢	٠.٩١	٢١.٣٢	٠.٩٤	٠.٠٠
٢. يساهم تخفيض مخاطر الأمن السيبراني في تعزيز رضا العاملين	٤.١٧	٠.١٤	٠.٨٦	٢١.٣٢	٠.٩٤	٠.٠٠
٣. يساهم تخفيض مخاطر الأمن السيبراني في تحسين سمعة البنك.	٤.٤٩	٠.١٦	٠.٨٩	٢١.٣٢	٠.٩٤	٠.٠٠
٤. يساهم تخفيض مخاطر الأمن السيبراني في دعم التتبع الإيجابي من الخبراء الماليين للبنك	٤.٥٨	٠.٠٩	٠.٩٠	٢١.٣٢	٠.٩٤	٠.٠٠
٥. يساهم تخفيض مخاطر الأمن السيبراني في جذب عملاء جدد	٤.٥٤	٠.١٢	٠.٨٨	٢١.٣٢	٠.٩٤	٠.٠٠
٦. يساهم تخفيض مخاطر الأمن السيبراني في زيادة إستخدام المواطنين للخدمات الإلكترونية.	٤.٦٩	٠.٠٩	٠.٨٤	٢١.٣٢	٠.٩٤	٠.٠٠
٧. يساهم تخفيض مخاطر الأمن السيبراني في تخفيض الجهود المبذولة لتنظيف أجهزة الكمبيوتر المصابة بالبرامج الضارة لشبكة الروبوتات.	٤.٦٢	٠.١١	٠.٩٢	٢١.٣٢	٠.٩٤	٠.٠٠
	٤.٥٣	٠.١٢	٠.٨٩	٢١.٣٢	٠.٩٤	٠.٠٠

يتبين من الجدول رقم (٧) أن قيمة الوسط الحسابي العام لمدى نتائج مدى تأثير المخاطر السيبرانية على الأداء غير المالي في البنوك التجارية المصرية بلغت (4.94) وبالمقارنة بالوسط الحسابي الفرضي البالغ (٣) كمعيار لقياس وتقييم الدرجة المتحصل عليها، وكذلك نتائج إختبار T لعينة واحدة ونتائج إختبار كولمجروف - سمرنوف والتي تشير لعدم وجود إختلافات جوهرية بين مفردات العينة، تم رفض فرض العدم وقبول الفرض البديل وهو: يوجد أثر ذو دلالة إحصائية للمخاطر السيبرانية على الأداء غير المالي في البنوك التجارية المصرية.

٦. الفرض السادس: لا يوجد أثر ذو دلالة إحصائية المخاطر السيبرانية على الأداء المالي وغير المالي في البنوك التجارية المصرية.

يبين لنا من نتائج الجدولين رقم (٦) ورقم (٧) نتائج مدى تأثير الإنفاق في الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية، من خلال الوسط الحسابي والإنحراف المعياري وإختبارT لعينة واحدة والأهمية النسبية.

جدول رقم (٨)

نتائج مدى تأثير المخاطر السيبرانية على الأداء المالي وغير المالي في البنوك التجارية المصرية.

البيان	الوسط الحسابي	الانحراف المعياري	الأهمية النسبية	قيمة (T) المحسوبة	كولمجروف - سمرنوف	مستوى المعنوية
متوسط نتائج مدى تأثير المخاطر السيبرانية على الأداء المالي في البنوك التجارية المصرية	٤.٨٨	٠.١١	٠.٩١	٢١.٣٢	٠.٩٤	٠.٠٠
متوسط نتائج مدى تأثير المخاطر السيبرانية على الأداء غير المالي في البنوك التجارية المصرية	٤.٥٣	٠.١٢	٠.٨٩	٢١.٣٢	٠.٩٤	٠.٠٠
المجموع	٤.٧١	٠.١٢	٠.٩٠	٢١.٣٢	٠.٩٤	٠.٠٠

تبين من الجدول رقم (٨) أن قيمة الوسط الحسابي لمدى مدى تأثير المخاطر السيبرانية على الأداء المالي وغير المالي في البنوك التجارية المصرية، بلغت (٤.٧١) وبالمقارنة بالوسط الحسابي الفرضي البالغ (٣) كمعيار لقياس وتقييم الدرجة المتحصل عليها، وكذلك نتائج إختبار T لعينة واحدة ونتائج إختبار كولمجروف - سمرنوف والتي تشير لعدم وجود إختلافات جوهرية بين مفردات العينة، تم رفض فرض العدم وقبول الفرض البديل وهو: يوجد أثر ذو دلالة إحصائية للمخاطر السيبرانية على الأداء المالي وغير المالي في البنوك التجارية المصرية.

٧. لا توجد إختلافات جوهرية بين آراء المبحوثين حول تأثير الإنفاق في الأمن السيبراني على المخاطر السيبرانية والأداء المالي وغير المالي في البنوك التجارية..

ولقياس عدم وجود إختلافات جوهرية بين آراء المبحوثين تم عمل إختبار كروسكال – والاس "Kruskal-Wallis Test" لإختبار جوهرية الإختلافات بين متوسطات فئات المبحوثين الثلاثة وكانت نتائج الإختبار كما هي موضحة في الجدول رقم (٩).

جدول رقم (٩)

نتائج عدم وجود إختلافات بين آراء المبحوثين حول تأثير الإنفاق في الأمن السيبراني على المخاطر السيبرانية والأداء المالي وغير المالي في البنوك التجارية

الفئات	العدد	متوسط الرتب	درجات الحرية	كا²	مستوى المعنوية
مدير فرع	٦٧	٦١.١	٣	٢.٥٦	٣.١٩
نائب مدير فرع	٥٢	٥٦.٣			
رئيس قسم	٦١	٥٨.٧			
مصرفي					
	١٨٠				

ويتبين من الجدول رقم (٩) نتائج التباين بين آراء المبحوثين في الفئات الأربعة عن طريق إختبار "Kruskal-Wallis Test" حيث كانت قيمة **كا²** (٢.٥٦) وهي أقل من مستوى المعنوية البالغ قدره (٣.١٩)، ومن هذا يتضح عدم وجود إختلاف بين آراء فئات عينة البحث، وبالتالي كانت آراء الفئات الأربعة من مديري ونواب مديري الفروع ومدراء الأقسام والمصرفيين العاملين بالبنوك، آراء متوافقة وهو ما يعضد نتائج البحث.

ويمكن ترتيب مدى تأثير الإنفاق في الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية المصرية، حسب درجة الأهمية النسبية كما هي موضحة في الجدول رقم (١٠).

جدول رقم (١٠)

ترتيب مدي تأثير الإنفاق في الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية المصرية

م	البيان	الوسط الحسابي	الأهمية النسبية	ترتيب الأهمية النسبية
١	أثر الإنفاق في المنع (الوقاية) والكشف عن الجرائم السيبرانية في تخفيض المخاطر السيبرانية في البنوك التجارية	٤.٥٧	٠.٩٤	١
٢	أثر الإنفاق في تطوير الأمن السيبراني في تخفيض المخاطر السيبرانية في البنوك التجارية	٤.٥٤	٠.٩٠	٢

ويتبين من الجدول رقم (١٠) الأهمية النسبية لدرجة تأثير الإنفاق في الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية المصرية، حيث جاء في الترتيب الأول أثر الإنفاق في المنع (الوقاية) والكشف عن الجرائم السيبرانية في تخفيض المخاطر السيبرانية في البنوك التجارية المصرية بمتوسط (٤.٥٧)، وفي الترتيب الثاني جاء أثر الإنفاق في تطوير الأمن السيبراني في تخفيض المخاطر السيبرانية في البنوك التجارية المصرية بمتوسط (٤.٥٤).

كما يمكن ترتيب مدى تأثير المخاطر السيبرانية على الأداء المالي وغير المالي في البنوك التجارية المصرية، حسب درجة الأهمية النسبية كما هي موضحة في الجدول رقم (١١).

جدول رقم (١١)

ترتيب مدي تأثير المخاطر السيبرانية على الأداء المالي وغير المال في البنوك التجارية المصرية

م	البيان	الوسط الحسابي	الأهمية النسبية	ترتيب الأهمية النسبية
١	أثر المخاطر السيبرانية على الأداء المالي في البنوك التجارية المصرية	٤.٨٨	٠.٩٤	١
٢	أثر المخاطر السيبرانية على الأداء المالي في البنوك التجارية المصرية	٤.٥٣	٠.٩٠	٢

ويتبين من الجدول رقم (١١) الأهمية النسبية لدرجة تأثير المخاطر السيبرانية على الأداء المالي وغير المالي في البنوك التجارية المصرية، حيث جاء في الترتيب الأول أثر المخاطر السيبرانية على الأداء المالي في البنوك التجارية المصرية بمتوسط (٤.٨٨)، وفي الترتيب الثاني جاء أثر المخاطر السيبرانية على الأداء غير المالي في البنوك التجارية المصرية بمتوسط (٤.٥٣).

٨. خلاصة ونتائج البحث ومقترحات لبحوث مستقبلة

١-٧ أولا: خلاصة البحث

تم تناول الإنفاق في الأمن السيبراني والمخاطر السيبرانية وتأثيرهم على الأداء المالي وغير المالي في البنوك التجالرية المصرية، فمخاطر الأمن السيبراني تؤدي إلى زيادة المخاطر التشغيلية التي تؤدي بدورها إلى ارتفاع التكاليف التشغيلية، وزيادة الإنفاق في الأمن السيبراني يساهم في تخفيض مخاطر الأمن السيبراني، وأن مخاطر الأمن السيراني كمتغير وسيط، تساهم في تحسين الأداء المالي وغير المالي في البنوك التجارية.

ويتكون الإنفاق على الأمن السيبراني من تكلفة المنع (الوقاية) والكشف عن الجرائم السيبرانية و تكلفة تطوير الأمن السيبراني، كما تتحمل البنوك خسائر ناتجة عن زيادة مخاطر الأمن السيبراني تتمثل في خسائر الاستجابة للجرائم السيبرانية والخسائر غير المباشرة، ولا شك أن الإنفاق في الأمن

السيبراني يساهم في تخفيض مخاطر الأمن السيبراني الأمر الذي سيكون له تأثير إيجابي على الأداء المالي وغير المالي للبنوك التجارية، كما أن إنخفاض الإنفاق في الأمن السيبراني يساهم في زيادة المخاطر السيبرانية، والتي تؤدي بدورها إلى زيادة الخسائر المدفوعة عن المخاطر السيبرانية.

وتم تحليل العلاقة بين الإستثمار في الأمن السيبراني والمخاطر السيبرانية والأداء في البنوك التجارية والعوامل التي ينبغي مراعاتها عند تحديد حجم الإنفاق في الأمن السيبراني، وكيف إدارة حجم الإنفاق في الأمن السيبراني في البنوك، ودور العائد على الإستثمار الأمني في إتخار القرار الإستثماري في الأمن السيبراني.

وأظهرت نتائج الدراسة الميدانية أن جميع المتغيرات المستقلة (الإنفاق في المنع والكشف عن الجرائم السيبرانية والإنفاق في تطوير الأمن السيبراني) كان لها أثر إيجابي في تخفيض المخاطر السيبرانية في البنوك التجارية، كما أن تخفيض المخاطر السيبرانية كان له أثر إيجابي على الأداء المالي وغير المالي في البنوك التجارية.

٢-٧ نتائج البحث

يمكن عرض النتائج التي توصل اليها البحث في النقاط الآتية:

من حيث قياس مدى تأثير الإنفاق في الأمن السيبراني على المخاطر السيبرانية والأداء المالي وغير المالي في البنوك التجارية المصرية جاءت نتائج الدراسة الميدانية على النحو التالي:

١. يوجد أثر ذو دلالة إحصائية لتكلفة المنع والكشف عن الجرائم السيبرانية على المخاطر السيبرانية في البنوك التجارية المصرية.
٢. يوجد أثر ذو دلالة إحصائية لتكاليف تطوير الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية المصرية.
٣. يوجد أثر ذو دلالة إحصائية للإنفاق في الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية المصرية.
٤. يوجد أثر ذو دلالة إحصائية للمخاطر السيبرانية على الأداء المالي في البنوك التجارية المصرية.
٥. يوجد أثر ذو دلالة إحصائية للمخاطر السيبرانية على الأداء غير المالي في البنوك التجارية المصرية.
٦. يوجد أثر ذو دلالة إحصائية للمخاطر السيبرانية على الأداء المالي وغير المالي في البنوك التجارية المصرية.
٧. ومن حيث الأهمية النسبية لمدي أثر الإنفاق في الأمن السيبراني على المخاطر السيبرانية في البنوك التجارية المصرية كانت النتائج على النحو التالي:
   - جاء في الترتيب الأول أثر الإنفاق في المنع (الوقاية) والكشف عن الجرائم السيبرانية في تخفيض المخاطر السيبرانية في البنوك التجارية المصرية بمتوسط (٤.٥٧)
   - جاء في الترتيب الثاني أثر الإنفاق في تطوير الأمن السيبراني في تخفيض المخاطر السيبرانية في البنوك التجارية المصرية بمتوسط (٤.٩٥).
٨. من حيث الأهمية النسبية لدرجة أثر المخاطر السيبرانية على الأداء المالي وغير المالي في البنوك التجارية المصرية كانت النتائج على النحو التالي:

- جاء في الترتيب الأول أثر المخاطر السيبرانية على الأداء المالي في البنوك التجارية المصرية بمتوسط (٤.٨٨)،
- جاء في الترتيب الثاني أثر المخاطر السيبرانية على الأداء غير المالي في البنوك التجارية المصرية بمتوسط (٤.٥٣).

٩. تلعب المخاطر السيرانية دوراً هاماً كمتغير وسيط بين الإنفاق في الأمن السيبراني والأداء في البنوك التجارية، حيث يؤدي الإنفاق في الأمن السيبراني إلى تخفيض المخاطر السيبرانية والتي بدورها تساهم في تحسين الأداء المالي وغير المالي للبنوك التجارية.

١٠. تم إجراء إختبار كروسكال – والاس "Kruskal-Wallis Test"وتبين عدم وجود إختلاف بين آراء فئات عينة البحث، وبالتالي كانت آراء الفئات الأربعة من مديري ونواب مديري الفروع ومدراء الأقسام والمصرفيين العاملين بالبنوك آراء متوافقة وهو ما يعضد نتائج البحث.

٣-٧ مقترحات بحوث مستقبلية:

بناءً على ما توصل إليه البحث من نتائج ومن خلال ما تم الإطلاع عليه من الدراسات السابقة يمكن إقتراح مجموعة من البحوث المستقبلية على سبيل المثال فيما يلي:

١. إجراء مزيد من الدراسات حول مجالات الإنفاق في الأمن السيبراني.
٢. إجراء مزيد من الدراسات حول مجالات المخاطر السيبرانية في البنوك التجارية.
٣. أثر الإنفاق في الأمن السيبراني على الأداء الاستراتيجي للمؤسسات غير المالية.
٤. إجراء دراسة تطبيقية لحساب العائد على الإستثمار الأمني في المؤسسات المالية وشركات الأعمال.
٥. أثر إفصاح الشركات عن تقرير إدارة مخاطر الأمن السيبرانى على العائد على الإستثمار الأمني.

المراجـع:

أولاً: المراجع باللغة العربية

- أبو موسى، أحمد عبد السلام، (٢٠٠٤)، أهمية مخاطر نظم المعلومات المحاسبية الإلكترونية، دراسة تطبيقية على المنشآت السعودية، مجلة التجارة والتمويل، كلية التجارة، جامعة طنطا، (٢): ١-٥٤.
- البغدادي، مروة فتحي السيد، (٢٠٢١)، إقتصاديات الأمن السيبراني في القطاع المصرفي، مجلة البحوث القانونية والإقتصادية، كلية الحقوق، جامعة المنصورة، (٧٦):١٤٦٦-١٥١٣.
- أرشيد، عقلة نواش محمد (٢٠١٧) أثر الاستثمار في تكنولوجيا المعلومات على أداء المصارف السعودية، المجلة العربية للإدارة، ٣٧ (١): ٢٠٧-٢٢٣.
- الرشيدي، طارق عبدالعظيم يوسف، والسيد، داليا عادل عباس، (٢٠١٩)، أثر الإفصاح عن مخاطر الأمن السيبراني في التقارير المالية على أسعار الأسهم وأحجام التداول: دراسة مقارنة في قطاع تكنولوجيا المعلومات. مجلة المحاسبة والمراجعة، (٢):٤٣٩-٤٨٧. مسترجع من /1122133Record/com.mandumah.search://h
- الركبان، الجوهرة بنت عثمان بن علي، (٢٠٢٣)، تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية: دراسة تقويمية، المجلة العربية للدراسات التربوية والاجتماعية، (٢٠) ١٥٩ - ٢٠٩ مسترجع من /http//:search.mandumah.com/Record1353685
- أميرهم، جيهان عادل، (٢٠٢٢)، أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وانعكاساته على ترشيد قرارات المستثمرين: دراسة ميدانية، مجلة البحوث المالية والتجارية، ٢٣(٣): ٣٢٥ - ٣٧٧ مسترجع من http//:search.mandumah.com/Record13
- بانقا، علم الدين، (٢٠١٩)، مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي، سلسلة دراسات تنموية، المعهد العربي للخطيط بالكويت،٦٣.
- حسان، محمد أمين روبين، (٢٠٢١)، أثر الاستثمار في تكنولوجيا المعلومات على الأداء المالي: دراسة تطبيقية على البنوك المدرجة في بورصة فلسطين، مجلة الجامعة الإسلامية للدراسات الاقتصادية والإدارية، ٣٠(١): ٨٣-١٠٩
- رشوان، عبد الرحمن محمد سليمان؛ وقاسم، زينب عبد الحفيظ أحمد، (٢٠٢٢)، أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك، المؤتمر العلمي الدولي الأول بعنوان "أثر الأمن السيبراني على الأمن الوطني خلال الفترة ٢٠ - ٢١ / ديسمبر/ ٢٠٢٢، جامعة عمان العربية بالاشتراك مع مديرية الأمن العام، ١:٢٨.
- شحاتة، شحاتة السيد، (٢٠٢٢)، نحو دور فاعل للمراجع الداخلي في إدارة مخاطر الأمن السيبراني في الشركات المقيدة بالبورصة المصرية، المجلة العلمية للدراسات والبحوث المالية والإدارية، ١٣(٢): ٢٦:٣٧
- صالح، نرمين محمد (محددات فعالية المراجعة الداخلية للأمن السيبراني)، ٢٠٢٢، المؤتمر العلمي الخامس لقسم المحاسبة والمراجعة (تحديات وافاق مهنة المحاسبة والمراجعة في القرن الحادي والعشرين) للفترة من (١١-١٠- ٢٠٢٢).

- صندوق النقد العربي، (٢٠١٩)، سلسلة موجز سياسات حول أمن الفضاء السيبراني في القطاع المصرفي، (٤).
- علي، محمود أحمد؛ وعلي، صالح علي، (٢٠٢٢)، أثر الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني على قرار الإستثمار بأسهم الشركات المقيدة بالبورصة المصرية: دراسة تجريبية، مجلة الإسكندرية للبحوث المحاسبية، كلية التجارةن جامعة الأسكندرية، ٦(٣):١-٤٨.
- قاسم، سامر أحمد، وإبراهيم، أيهم يوسف، (٢٠٢٢)، دور تكنولوجيا المعلومات في تحسين كفاءة الابتكارات المصرفية: دراسة ميدانية على المصارف العامة في محافظة اللاذقية، مجلة جامعة تشرين للبحوث والدراسات العلمية، سلسلة العلوم الاقتصادية والقانونية، ٤٤(٢): ١٤٩ - ١٦٨ مسترجع من
- Record/com.mandumah.search://h١٢٦٩٩١١/
- محروس، رمضان عارف رمضان، وصالح، أبوالحمد مصطفى ،(٢٠٢٢)، استخدام المنهجية الرشيقة في تطوير أداء المراجعة الداخلية لمواجهة مخاطر الأمن السيبراني، مجلة البحوث المالية والتجارية، ٢٣(٣): ٤٣٢:٤٩١
- يعقوب، ابتهاج، وهاب، اسعد، والفرطوسي، على، (٢٠٢٢)، مؤشر مقترح للإفصاح المحاسبي عن المخاطر السيبرانية في سوق العراق للأوراق المالية على وفق المتطلبات الدولية: دراسة اختبارية، مجلة الدراسات المالية والمحاسبية والإدارية، ٩(١):١٤٠٣-١٤٣٠.
مسترجع من https://www.asjp.cerist.dz/en/article/192579

ثانياً: المراجع الأجنبية

- Agboola, A. (2007). Information and communication technology (ICT) in banking operations in Nigeria–An evaluation of recent experiences. African Journal of Public Administration and Management, 18(1), 1-102.
- AIG. (2016, December). Is Cyber Risk Systemic? New York: American International Group. Retrieved from https://www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/aigcyber-risk-systemic-final.pdf
- Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020a). Operational and cyber risks in the financial sector. BIS Working Paper No. 840. Basel, Switzerland: Bank for International Settlements.
- Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020b). The drivers of cyber risk. BIS Working Paper No. 865. Basel, Switzerland: Bank for International Settlements.
- Alqahtani, F. H. (2017). Developing an information security policy: A case study approach. Procedia Computer Science, 124, 691-697.

- Altobishi, T., Erboz, G., & Podruzsik, S. (2018). E-Banking effects on customer satisfaction: The survey on clients in Jordan Banking Sector. International Journal of Marketing Studies, 10(2), 151-161. https://doi.org/10.5539/ijms.v10n2p151
- Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M. & Savage, S. (2013). Measuring the cost of cybercrime. In The economics of information security and privacy (pp. 265-300).
- Archie, Jackson,(2023), Does RoSI (on Security Investment) analysis help in decision making؟ , Stay Aware | Stay Secure, A Cyber Security Newsletter, https://2u.pw/kMR8pQ4
- Ashford, W. (2019, July 31). Financial services top cyber attack target. Computer Weekly. Retrieved from https://www.computerweekly.com
- Badawy, H. (2021) . The Impact of Assurance Quality and Level on Cybersecurity Risk Management Program on Non-Professional Egyptian Investors' Decisions: An Experimental Study. Alexandria Journal of Accounting Research.3 (5):1-56.
- BDO. (2017). cyber security in banking industry. India: BDO.
- BIS. (2016, june). Bank for International Settlements. Retrieved from www.bis.org: https://www.bis.org/cpmi/publ/d146.pdf
- Boin, A., & McConnell, A. (2007). Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. Journal of Contingencies and Crisis Management, 15(1):50-59.
- Bokhari, S. A. A., & Manzoor, S. (2022). Impact of information security management system on firm financial performance: perspective of corporate reputation and branding. American Journal of Industrial and Business Management, 12(5), 934-954.
- Bouveret, A. (2018). Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment. IMF Working Paper No. WP/18/143. International Monetary Fund
- Brechbuhl, H., Bruce, R., Dynes, S., & Johnson, M. E. (2010). Protecting Critical Information Infrastructure: Developing Cybersecurity Policy. Information Technology for Development, 16(1), 83-91.

- CarlColwill. (2009). Human factors in information security: The insider threat – Who can you trust these days? Information Security Technical Report, 14(4), 186-196.
- Cheng, X., Hsu, C., & Wang, T. D. (2022). Talk too much? The Impact of Cybersecurity Disclosures on Investment Decisions. Communications of the Association for Information Systems, 50 (1), 26
- Columbus, L. (2020). Top 10 Cyber Security companies to watch in 2020 https://www.forbes.com/sites/louiscolumbus/2020/01/26/top-10-CyberSecurity-companies-to-watch-in2020/#3d820fd24fe6
- Desta, N. D. (2016). Information safety, corporate image, and intention to Use online services: Evidence from travel industry in Vietnam.
- Desta, Y. (2018). Customers' e-banking adoption in Ethiopia, PhD Dissertation, Addis Ababa University, Ethiopia.
- Donge, Z., Luo, F., & Liang, G. (2018). Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems. Journal of Modern Power Systems and Clean Energy, 1-10.
- Eling, M., & Lehmann, M. (2018). The Impact of Digitalization on the Insurance Value Chain and the Insurability of Risks. The Geneva Papers on Risk and Insurance-Issues and Practice, 43(3), 359- 396.
- Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? European Journal of Operational Research, 272(3), 1109-1119.
- Euromoney. (2017, August 1). Technology investments drive up banks' costs. Euromoney magazine. London.
- EU. (2018, May). The Directive on security of network and information systems (NIS Directive). Retrieved from https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
- Fed. (2017, September). Federal Reserve Policy on Payment System Risk. Washington, USA: Federal Reserve System. Electronic copy available at: https://ssrn.com/abstract=3689162

- Fitch. (2017, April). Cybersecurity an Increasing Focus for Financial Institutions. Retrieved from https://www.fitchratings.com/site/pr/1022468
- Gatzert, N., & Schubert, M. (2022). Cyber risk management in the US banking and insurance industry: A textual and empirical analysis of determinants and value. Journal of Risk and Insurance, 89(3), 725-763..
- Germano, J. H. (2014). Cybersecurity Partnerships: A New Era of Public-Private Collaboration. New York: New York University School of Law.
- Gladstone, R. (2016, March 15). Bangladesh Bank Chief Resigns After Cyber Theft of $81 Million. The New York Times.
- Geyres, S., & Orozco, M. (2016). Think banking cybersecurity is just a technology issue? Think again. accenture strategy. Retrieved from https://www.accenture.com/t20160419t004021__w__/usen/_acnmedia/pdf-13/accenture-strategy-cybersecurity-in-banking.pdf
- Gopalakrishnan, R., & Mogato, M. (2016, May 19). Bangladesh Bank official's computer was hacked to carry out $81 million heist: diplomat. Reuters: Business News. Thomson Reuters
- Gordon, L. A., & Loeb, M. P. (2002a). The economics of information security investment. ACM Transactions on Information and Systems Security, 5(4), 438-457.
- Gordon, L. A., & Loeb, M. P. (2002b). Return on information security investments, myths vs realities. Strategic Finance, 84(5), 26-31.
- Johnson, K. N. (2015). Managing Cyber Risk. Georgia Law Review , 50(2), 548-592.
- Juma'h, A. H., & Alnsour, Y. (2020). The effect of data breaches on company performance. International Journal of Accounting & Information Management, 28(2), 275-301.
- Kamiya, S., KangJun-Koo, Jungmin, K., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms . Journal of Financial Economics, In Press.
- Kark, K., Shaikh, A., & Brown, C. (2017, November 28). Technology budgets: From value preservation to value creation. Deloitte Insight. London.

- Khalil, K., Usman, A., & Manzoor, S. R. (2020). Effect of cyber security costs on performance of E-banking in Pakistan. Journal of Managerial Sciences, 14. 26-40
- Kejwang, B. (2022). Effect of cybersecurity risk management practices on performance of insurance sector: A review of literature. International Journal of Research in Business and Social Science (2147-4478), 11(6), 334-340
- Kesswani, N., & Kumar, S. (2015). Maintaining Cyber Security: Implications, Cost and Returns. Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research (pp. 161- 164, New York: Association for Computer Machinery
- Khalil, K. (2020). Effect of cyber security costs on performance of e-banking in Pakistan. Journal of Managerial Sciences, 14(4), 85-99.
- Khalil, K., Usman, A., & Manzoor, S. R. (2020). Effect of cyber security costs on performance of E-banking in Pakistan. Journal of Managerial Sciences, 14. 26-40.
- Khalid Khalil, Sheikh Raheel Manzoor , Muhammad Tahir , Nisar Khan , Khalid Jamal,(2021),MPACT OF CYBER SECURITY COST ON THE FINANCIAL PERFORMANCE OF E-BANKING: MEDIATING INFLUENCE OF PRODUCT INNOVATION PERFORMANCE, Humanities & Social Sciences Reviews, 9(2): pp 691-703 https://doi.org/10.18510/hssr.2021.9266
- Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber Risk, Market Failures, and Financial Stability, Working Paper. International Monetary Fund (WP/17/185).
- Kox, H. L. (2013). Cybersecurity in the perspective of Internet traffic growth. Working paper. CPB Netherlands Bureau for Economic Policy Analysis. Retrieved from https://mpra.ub.unimuenchen.de/47994/
- Lewis, J., & Baker, S. (2013). The Economic Impact of Cybercrime and Cyber Espionage. McAfee.
- Lever, K. E., & Kifayat, K. (2020). Identifying and mitigating security risks for secure and robust NGI networks. Sustainable Cities and Society, 59, 102098.
- Low, P. (2017). Insuring against cyber-attacks. Computer Fraud & Security (4), 18-20.

- Macaulay, T. (2018). Critical Infrastructure:Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies (1st ed.). Boca Raton: Taylor and Francis Group.
- Moore, T., Clayton, R., & Anderson, R. (2010). The economics of online crime. The Journal of Economic Perspectives, 23(3), 3-20.
- Nazaritehrani, A., & Mashali, B. (2020). Development of E-bankingchannels and market share in developing countries. Financial Innovation, 6(1), 12. https://doi.org/10.1186/s40854-020-0171-z
- Ni, J., Lin, X., & Shen, X. (. (2019). Towards Edge-assisted Internet of Things: From Security and Efficiency Perspectives. IEEE Network, 33(2), 50-57
- .Njoroge, E. W. (2017). Effect of cyber security related costs ondevelopment of product innovation performances and services: A case study of NIC bank of Kenya. PhD Dissertation. Kenyatta University of Agriculture and Technology.
- .Njoroge, E., & Njeru, A. (2017). The effect of cybercrime response costs for the development of financial products: A case of NIC bank of Kenya. Journal of Managerial Sciences, 14(2),33-51.
- Njoroge, M. N., & Mugambi, F. (2018). Effect of electronic banking on financial performance in Kenyan commercial banks: Case of equity bank in its Nairobi central business district branches, Kenya. International Academic Journal of Economics and Finance, 3(2), 197-215.
- Njogu, N. J. (2014). "The Effect of Electronic Banking on Profitability of Commercial Banks in Kenya". Master of Science in Finance, School Of Business, University Of Nairobi
- OFR. (2017). Cybersecurity and Financial Stability: Risks and Resilience. Office of Financial Research.
- Padmaavathy, P. A. (2019). Cyber Crimes: A Threat To The Banking Industry. International Journal of Management Research and Reviews, 9(4), 1-9.
- Page, J., Kaur, M., & Waters, E. (2017). Directors' liability survey: Cyber attacks and data loss — a growing concern. Journal of Data Protection & Privacy, 1(2), 173-182.

- Paul, J. A., & Wang, X. (2019). Socially optimal IT investment for cybersecurity. Decision Support Systems, 122, 113069.
- Peng, C., Xu, M., Xu, S., & Hu, T. (2017). Modeling and predicting extreme cyber attack rates via marked point processes. Jornal of Applied Statistics, 44(14), 2534-2563
- Sandhu, S., & Arora, S. (2021). Customers' usage behaviour of e-banking services: Interplay of electronic banking and traditional banking. International Journal of Finance & Economics, 27(2), 2169-2181. https://doi.org/10. 1002/ijfe.2266
- Schwartz, M. J. (2013, March 21). South Korea Bank Hacks: 7 Key Facts. Dark Reading. Retrieved from https://www.darkreading.com
- Security Scoreboard. (2016). Financial Industry Cybersecurity Report. New York: Security Scoreboard.
- Skinner, D. j., & Sloan, R. G. (2002). Earnings Surprises, Growth Expectations, and Stock Returns or Don't Let an Earnings Torpedo Sink Your Portfolio. Review of Accounting Studies, 7, 289–312.
- Söylemez, S. A., & Ahmed, A. H. (2019). The role of new economic indicators on banking sector performance in Ghana: Trend and empirical research, analysis of banks' clients and experts perception. Journal of Finance and Economics, 7(1), 23-35.
- Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. Decision Support Systems(75), 49–62.
- Sulaiman, N., Hamdan, A., & Al Sartawi, A. (2022). The Influence of Cybersecurity on the Firms' Financial Performance. In Future of Organizations and Work After the 4th Industrial Revolution: The Role of Artificial Intelligence, Big Data, Automation, and Robotics (pp. 443-461). Cham: Springer International Publishing.
- Trautman, L. J., & Altenbaumer-Price, K. (2010). The board's responsibility for information technology governance. J. Marshall J. Computer & Info. L, 28, 313.
- Toivanen, H. (2015). Case study of why information security investment fail?. Master's Thesis, 76. Jyväskylä, Finland: University of Jyväskylä

- Vagle, J. (2020). Cybersecurity and Moral Hazard. Stanford Technology Law Review, 23,

ثالثاً: الروابط

- https://cutt.us/6H4AY
- https://www.business.com/articles/smb-budget-for-cybersecurity/
- https://2u.pw/c5zCUHL
- https://2u.pw/q3GBHJG
- https://2u.pw/1GGhOtD, Return on Security Investment (RoSI): The Full Guide. Security Management / January 9, 2023
- https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/hit-or-myth-understanding-the-true-costs-and-impact-of-cybersecurity-programs
- https://www.sentinelone.com/blog/a-cyberwar-on-financial-institutions-why-banks-are-caught-in-the-crosshairs/
- https://www.nedigital.com/en/blog/financial-and-reputational-benefits-of-a-cyber-security-management-plan
- https://2u.pw/qwO1wbZ , How to Calculate Your Return On Security Investments: FP&A's Role ,By Bryan Lapidus, FPAC. Published: 10/16/2018>

قائمة استقصـــــــــــــاء

يقوم الباحث بإعداد بحث بعنوان: " أثر الإنفاق في الأمن السيبراني على الأداء في البنوك التجارية المصرية مع دراسة ميدانية" ، ويهدف هذا البحث إلى بيان مدى تأثير الإنفاق في الأمن السيبراني على الأداء المالي وغير المالي في البنوك التجارية المصرية، وتم توسيط متغير المخاطر السيبرانية، حيث يتم أولاً دراسة مدى تأثير الإنفاق في الأمن السيبراني على تخفيض المخاطر السيبرانية، ثم دراسة مدى تأثير تخفيض المخاطر السيبرانية على الأداء المالي وغير المالي في البنوك التجارية المصرية، ونظراً لأن قيمة ونجاح أي بحث علمي لا يتحقق إلا من خلال ربط الجانب الأكاديمي والجانب التطبيقي، لذا فإن الباحث يحاول من خلال قائمة الإستقصاء أو الإستبيان معرفة وجهة نظر سيادتكم في الأمور الواردة بالقائمة .

ويؤكد الباحث على أن مساهماتكم في هذا البحث عن طريق تخصيص جزء من وقتكم الثمين وإمدادنا بالبيانات المطلوبة، لأن ذلك هو الأساس الذى سيترتب علية نجاح هذا البحث ونؤكد لسيادتكم أن هذه البيانات لن تستخدم إلا في أغراض البحث العلمي فقط.

ويشكر الباحث سيادتكم جزيل الشكر لحسن تعاونكم معه في العمل على خدمة وإنجاح هذا البحث العلمي.

اسم الباحث

عبدالعال مصطفى ابو الفضل

استاذ المحاسبة المساعد

أولاً : البيانات الشخصية : كان مجتمع البحث المستهدف موظفي الكادر الإداري في البنوك التجارية في مصر

المسمى الوظيفي : مدير فرع ☐ رئيس قسم ☐ مصرفي ☐

عدد سنوات الخبرة: : ٥-١٠ ☐ ١٠- ١٥ ☐ ١٥-٢٠ ☐ أكثر من ٢٠ ☐

المؤهل العلمي : بكالوريوس ☐ ماجستير ☐ دكتوراه ☐ أخرى(تذكر) ☐

ثانياً : مفاهيم :

- المخاطر السيبرانية : وتتمثل مخاطر الأمن السيبراني في المخاطر التكنولوجية والتشغيلية والتنظيمية التي تتعرض لها المنشآت المعتمدة على تقنيات تكنولوجيا المعلومات والناتجة عن اختراق نظام الأمن السيبراني لديها بما يحد من قدرة البنوك على تحقيق أهدافها.
- الأمن السيبراني: يهتم بتصميم وتطبيق التقنيات والعمليات والضوابط والممارسات اللازمة لحماية الأنظمة والشبكات والبرامج والأجهزة والبيانات في البنوك من التعرض للهجمات والتهديدات الإلكترونية والفيروسات وسد ثغرات نقاط الضعف المباشرة أو غير المباشرة.

- الإستثمار في الأمن السيبراني: هو تكاليف الإنفاق على الأمن السيبراني المتمثل في تكلفة المنع (الوقاية) والكشف عن الجرائم السيبرانية وتكلفة تطوير الأمن السيبراني.

السؤال الأول: تساهم الإنفاق في المنع (الوقاية) والكشف عن الجرائم السيبرانية في تخفيض المخاطر السيبرانية في البنوك التجارية من خلال الوسائل التالية:

م	الفقرات	موافق تماماً	موافق	محايد	غير موافق	غير موافق تماماً
١	تساهم تكاليف أنظمة أمن تكنولوجيا المعلومات مثل مرشحات البريد العشوائي وجدران الحماية وبرامج مكافحة الفيروسات وملحقات المتصفح لحماية المستخدمين في تخفيض المخاطر السيبرانية في البنوك التجارية.					
٢	تساهم تكاليف التأمين للأمن السيبراني في تخفيض المخاطر السيبرانية في البنوك التجارية.					
٣	تساهم التكاليف المرتبطة بالامتثال لمعايير تكنولوجيا المعلومات المطلوبة في تخفيض المخاطر السيبرانية في البنوك التجارية.					
٤	تساهم التكاليف الصيانة والتدابير الوقائية للأمن السيبراني في تخفيض المخاطر السيبرانية في البنوك التجارية.					

السؤال الثاني: تساهم الإنفاق في تطوير الأمن السيبراني في تخفيض المخاطر السيبرانية في البنوك التجارية من خلال الوسائل التالية:

م	الفقرات	موافق تماماً	موافق	محايد	غير موافق	غير موافق تماماً
١	تساهم تكاليف فحص الثغرات الأمنية في تخفيض المخاطر السيبرانية في البنوك التجارية					
٢	تساهم تكاليف إختبار الاختراق في تخفيض المخاطر السيبرانية في البنوك التجارية					
٣	تساهم تكاليف عمليات مراجعة أمن البيانات في تخفيض المخاطر السيبرانية في البنوك التجارية.					

م	الفقرات	موافق تماماً	موافق	محايد	غير موافق	غير موافق تماماً
٤	تساهم تكاليف تزويد الموظفين بالمعرفة والمهارات الحديثة اللازمة لمنع انتهاكات البيانات في تخفيض المخاطر السيبرانية في البنوك التجارية					

السؤال الثالث: يساهم تخفيض المخاطر السيبرانية في تحسين الأداء المالي في البنوك التجارية من خلال الوسائل التالية:

م	الفقرات	موافق تماماً	موافق	محايد	غير موافق	غير موافق تماماً
١	يساهم تخفيض مخاطر الأمن السيبراني في زيادة قيمة السوقية لأسهم البنك					
٢	يساهم تخفيض مخاطر الأمن السيبراني في تخفيض قيمة التعويضات المدفوعة					
٣	يساهم تخفيض مخاطر الأمن السيبراني في تخفيض قيمة الغرامات التنظيمية					
٤	يساهم تخفيض مخاطر الأمن السيبراني في تخفيض التكاليف القانونية					
٥	يساهم تخفيض مخاطر الأمن السيبراني في تخفيض تكاليف الاستجابة للتعافي من الكوارث.					
٦	يساهم تخفيض مخاطر الأمن السيبراني في تخفيض تكاليف استمرارية الأعمال.					
٧	يساهم تخفيض مخاطر الأمن السيبراني في زيادة ربحية البنك.					
٨	يساهم تخفيض مخاطر الأمن السيبراني في زيادة معدل العائد على الإستثمار في البنك.					
٩	يساهم تخفيض مخاطر الأمن السيبراني في زيادة معدل العائد على حقوق الملكية في البنك					

السؤال الرابع: يساهم تخفيض المخاطر السيبرانية في تحسين الأداء غير المالي في البنوك التجارية من خلال الوسائل التالية:

م	الفقرات	موافق تماماً	موافق	محايد	غير موافق	غير موافق تماماً
1	يساهم تخفيض مخاطر الأمن السيبراني في تعزيز رضا العملاء					
2	يساهم تخفيض مخاطر الأمن السيبراني في تعزيز رضا العاملين					
3	يساهم تخفيض مخاطر الأمن السيبراني في تحسين سمعة البنك.					
4	يساهم تخفيض مخاطر الأمن السيبراني في دعم التتبع الإيجابي من الخبراء الماليين للبنك					
5	يساهم تخفيض مخاطر الأمن السيبراني في جذب عملاء جدد					
6	يساهم تخفيض مخاطر الأمن السيبراني في زيادة إستخدام المواطنين للخدمات الإلكترونية.					
7	يساهم تخفيض مخاطر الأمن السيبراني في تخفيض الجهود المبذولة لتنظيف أجهزة الكمبيوتر المصابة بالبرامج الضارة لشبكة الروبوتات.					