Tikrit Journal of Administrative and Economic Sciences, Vol. 21, No. 72, Part (2): 60-77
Doi: www.doi.org/10.25130/tjaes.21.72.2.4

Tikrit Journal of Administrative and Economics Sciences
مجلة تكريت للعلوم الإدارية والاقتصادية
EISSN: 3006-9149
PISSN: 1813-1719

The economics of Cybersecurity and its impact on financial and banking risk management

Zahida Ali Yaseen Al-Barzanji*
Administrative Technical College/Northern Technical University

Abstract: The research aims to highlight and clarify the concept of Cybersecurity economics and its effective role in protecting banks and financial institutions from cyber-attacks. The research seeks to understand the practical reality of Cybersecurity economics and its impact on reducing banking risks in the branches of Al-Tayf Islamic Bank operating in Iraq. The research problem lies in the light of a number of the following questions: To what extent is Cybersecurity linked to methods of reducing financial and banking risks? To what extent does Cybersecurity affect mitigating these risks?. Both of quantitative and descriptive approaches were adopted in the analysis. A questionnaire was designed and distributed to a sample of (200) administrators and technicians in the Islamic Spectrum Bank and a number of its branches, who represent the study community. The research reached a number of results and recommendations, perhaps the most important of which is the existence of an influential relationship between the variable of Cybersecurity economics in mitigating banking risks. It recommended the need to focus on the presence of experts specializing in the field of Cybersecurity, and to work on attracting and appointing them in banks and financial institutions. And to benefit from their skills and scientific and technical capabilities in identifying potential internal and external risks.

Keywords:
Cybersecurity, Risk Management, Financial and Banking Risks, Al-Taif Islamic Bank.

A R T I C L E I N F O

Article history:

Received	17 Aug. 2025
Received in revised form	27 Sep. 2025
Accepted	02 Oct. 2025
Available online	31 Dec. 2025

*Corresponding author:
Zahida Ali Yaseen Al-Barzanji
Administrative Technical College/ Northern Technical University

Tikrit Journal of Administrative and Economic Sciences, Vol. 21, No. 72, Part (2): 60-77
Doi: www.doi.org/10.25130/tjaes.21.72.2.4

اقتصاديات الامن السيبراني وتأثيره في إدارة المخاطر المالية والمصرفية

زاهدة علي ياسين البرزنجي
الجامعة التقنية الشمالية الكلية التقنية الادارية

المستخلص

عمل البحث على ابراز وتوضيح لمفهوم اقتصاديات الأمن السيبراني ودورها الفعال في حماية المصارف والمؤسسات المالية من الهجمات السيبرانية، وهدف البحث إلى معرفة الواقع التطبيقي لاقتصاديات الامن السيبراني وأثره في الحد من المخاطر المصرفية في فروع مصرف الطيف الاسلامي العاملة في العراق، تكمن مشكلة البحث في ضوء عدد من الأسئلة الآتية: إلى أي مدى يرتبط الأمن السيبراني مع أساليب الحد من المخاطر المالية والمصرفية؟ وإلى أي مدى يؤثر الأمن السيبراني في الحد من هذه المخاطر؟، ولقد تم اعتماد المنهج الكمي والمنهج الوصفي في التحليل، وقد صممت الاستبانة ووزعت على عينة مكونة من 200 من الإداريين والفنيين في مصرف الطيف الاسلامي وعدد من فروعه الذين يمثلون مجتمع الدراسة. خرج البحث بعدد من النتائج والتوصيات لعل أهمها هو وجود علاقة تأثيرية لمتغير اقتصاديات الامن السيبراني في الحد من المخاطر المصرفية، وأوصى بضرورة التركيز على وجود خبراء متخصصين في مجال الأمن السيبراني، والعمل على استقطابهم وتعيينهم في المصارف والمؤسسات المالية، والاستفادة من مهاراتهم وقدراتهم العلمية والمهارية في تحديد المخاطر الداخلية والخارجية المحتملة.

الكلمات المفتاحية: الأمن السيبراني، إدارة المخاطر، المخاطر المالية والمصرفية، مصرف الطيف الإسلامي.

المقدمة

ليس بعيداً عن الادراك فقد أصبح واضحاً إن التكنولوجيا والاتصالات هي البنية التحتية الأساسية لهذا النظام المالي العالمي الجديد، لذلك تحرص العديد من المصارف والمؤسسات المالية على تبني الخدمات المالية الرقمية والاستفادة منها لتكون أكثر قدرة على المنافسة، فضلاً عن تقليل التكلفة وتحقيق الكفاءة المؤسسية لمواكبة الساحة الجديدة والاستمرار فيها. لذلك يتطلب الأمر بذل جهود جادة لإنشاء بنية تحتية قوية ومرنة عبر الإنترنت، وهذا ما أدركته الكثير من المصارف والمؤسسات المالية العالمية بعامة والعراقية بخاصة، ذلك إن الاضطلاع بدور قيادي في تطوير إطار عمل للأمن السيبراني يُتيح فهماً أعمق لمشهد التهديدات، ويُحدد متطلبات ضمان المرونة السيبرانية. ومن الضروري للبنوك والمؤسسات المالية مواكبة التطورات التكنولوجية للحفاظ على مرونة عالية في مواجهة أحدث الهجمات السيبرانية وأكثرها تطوراً، وهذا يتطلب من العاملين في هذه المؤسسات الاهتمام بشكل أكبر بعملية إدارة المخاطر المالية والمصرفية، إن الدور القيادي في تطوير إطار الأمن السيبراني يوافر فهماً أفضل لمشهد التهديدات، ويحدد المتطلبات اللازمة لضمان المرونة السيبرانية، ومن الضروري أن تواكب هذه المصارف والمؤسسات المالية التطورات التكنولوجية لضمان قدرتها العالية على الصمود في وجه أحدث الهجمات الإلكترونية وأكثرها تطوراً. وهذا يتطلب من العاملين في هذه المؤسسات إيلاء اهتمام أكبر لعملية إدارة المخاطر المالية والمصرفية، وفهم مفهومها وأسبابها وأثرها في تقليل الخسائر في هذه المؤسسات، وبالتالي تحقيق الربحية اللازمة لدخول أسواق جديدة ومنافسة البنوك والمؤسسات المالية الأخرى.

مشكلة البحث: تكمن مشكلة البحث في ضوء عدد من الأسئلة الآتية: إلى أي مدى يرتبط الأمن السيبراني مع أساليب الحد من المخاطر المالية والمصرفية؟ وإلى أي مدى يؤثر الأمن السيبراني في الحد من هذه المخاطر؟ وما هي وسائل الأمن السيبراني أو عناصره التي تسهم في الحد من هذه المخاطر؟

أهمية البحث: تأتي أهمية البحث من كونه إلقاء الضوء على الدور المنوط بالمؤسسات المالية والمصرفية في عصر تسوده العولمة الإلكترونية حتى تخرج من النمط الكلاسيكي إلى النمط الحديث القائم على التصدي لهذه الظاهرة الخطيرة والوقاية منها، لهذا تتجلى أهمية الأمن السيبراني وتأثيره في إدارة المخاطر المالية والمصرفية لهذه المؤسسات مادياً وبشرياً وتجنب حدوثها في المصارف العراقية.

هدف البحث: يهدف البحث إلى التعرف على الواقع التطبيقي لاقتصاديات الأمن السيبراني وأثرها في الحد من المخاطر المالية والمصرفية في المصارف والمؤسسات المالية العاملة في العراق، ومعرفة الخلفية العلمية المتوافرة حول مفهوم الأمن السيبراني ومدى الوعي بمتطلباته سواء أكانت علمية أم معرفية لدى العاملين فيها.

فرضيات البحث: من أجل التوصل إلى حل منطقي لمشكلة البحث فقد تم وضع الفرضية الآتية: يوجد أثر ذو دلالة احصائية لاقتصاديات الأمن السيبراني في الحد من المخاطر في المؤسسات المالية والمصارف العاملة في العراق عند مستوى معنوية (0.05)، ويتفرع عنها الفرضيتين الآتيتين:

1. يوجد أثر ذو دلالة احصائية معنوية للموارد والامكانيات المادية والعلمية المتوافرة لدى المؤسسات المالية والمصرفية في الحد من المخاطر لهذه المؤسسات العاملة في العراق عند مستوى معنوية (0.05).
2. يوجد أثر ذو معنوية احصائية معنوية للموارد والامكانيات البشرية المتوافرة لدى المؤسسات المالية والمصرفية في الحد من المخاطر لهذه المؤسسات العاملة في العراق عند مستوى معنوية (0.05).

متغيرات البحث

1. المتغير المستقل: اقتصاديات الامن السيبراني، ويضم متغيرين مستقلين فرعيين هما الموارد والامكانيات المادية والعلمية والموارد والامكانيات البشرية.
2. المتغير التابع: الحد من المخاطر المالية والمصرفية.

المبحث الأول: الأمن السيبراني والمخاطر المالية والمصرفية

أ. **الأمن السيبراني:** عندما ضربت جائحة كورونا الأخيرة فقد تسارعت رقمنة القطاع المصرفي حول العالم، ومنذ ذلك الحين كانت الحضور في ميادين العمل قد انخفض، وقد صحب ذلك ارتفاعاً في استخدام الخدمات المصرفية عبر أجهزة الهاتف المحمول، لكن مع توقُّع الزبائن لتوافر خدمات سلسة وبتكلفة منخفضة مترافقة مع تحسين مستمر في الأداء، فقد ظهر ما يعرف بالخدمات المصرفية المفتوحة التي تسمح بتبادل ضخم للبيانات بين المصارف ومزوّدي الخدمات المالية من الطرف الثالث للابتكار، فضلاً عن تحسين تجربة الزبون وتقديم قيمة أعلى له، لكن نتيجة لذلك فقد ارتفع عدد الهجمات السيبرانية وبشكل ملحوظ، فبحسب ما جاء في مجلة الجرائم الإلكترونية Cybercrime Magazine في العدد الثالث عشر من عام 2020 فأن هذا النوع من الجرائم سيكلّف العالم نحو 10.5 تريليون دولار مع نهاية عام 2025.

يمكن تعريف الأمن السيبراني وفقاً لما ورد في التقرير الصادر عن الاتحاد الدولي للاتصالات حول "اتجاهات الاصلاح في الاتصالات للعام 2010-2011 بأنه مجموعة من المهمات، من مثل تجميع وسائل، وسياسات، واجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين". أما من حيث استناداً لأهدافه فيمكن تعريفه بأنه" النشاط الذي يؤمن حماية الموارد البشرية، والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويتضمن امكانات الحد من الخسائر والاضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح اعادة الوضع الى ما كان عليه، بأسرع وقت ممكن، بحيث لا تتوقف عجلة الانتاج، وبحيث لا تتحول الاضرار الى خسائر دائمة (البغدادي، 2020: 1453).

يعتمد الأمن السيبراني للمعلومات على ثلاثة محاور رئيسة لابد من توافرها في المعلومات التي تستوجب الحماية، وهي (الفوال، 2020: 12):

1. السرية: تتمثل السرية في القدرة على الحفاظ المعلومات وعدم تسربها، وذلك عن طريق منع الدخول غير المصرح للمعلومات سواء أكانت محفوظة على وسيط مادي أم يتم إرسالها عبر وسائل الاتصالات، والتأكد من عدم الإفصاح عنها فضلا عن عدم السماح بالاطلاع عليها إلا من خلال الأشخاص المصرح لهم بذلك.
2. سلامة المعلومات وتكامل المحتوى: وهو التأكد من المحافظة على محتوى المعلومات وسلامتها من العبث أو التعديل أو الإفساد، وذلك عن طريق منع الوصول إلى هذا المحتوى عن طريق التدخل غير المشروع.
3. توافر المعلومات وإتاحتها: وهو ضمان توافر المعلومات والقدرة على تقديمها وإتاحتها في الوقت المناسب من خلال الأشخاص المصرح لهم بذلك، والتأكد من أن هؤلاء الأشخاص لن يتم منعهم من استخدام المعلومات أو الدخول إليها.

أشار الباحثون إلى وجود خمسة أنواع أساسية من التهديدات السيبرانية وبخاصة تلك التي يمكن للمنظمة تحقيق أهدافها الامنية فيما لو تم تجاوزها أو تلافيها، وهذه التهديدات تتمثل في القرصنة السيبرانية والجريمة السيبرانية والتجسس السيبراني والإرهاب السيبراني والحرب الإلكترونية (Ahokas et al., 2017: 348).

يعاني الأمن السيبراني عدداً من التحديات الاقتصادية المتمثلة في الحوافز المنحرفة، وعدم تناسق المعلومات، والعوامل الخارجية، ومن ثم فإنه لا بد من أن تكون الخيارات التنظيمية متاحة للتغلب على هذه الحواجز في سياق الأمن السيبراني، التي تشتمل على تنظيم السلامة المسبق، والمسؤولية اللاحقة، والإفصاح عن المعلومات، ومسؤولية الوسيط غير المباشر.

لذلك لابد من وجود خيارات تنظيمية متاحة للتغلب على هذه الحواجز في سياق الأمن السيبراني التي تشمل تنظيم السلامة المسبق، والمسؤولية اللاحقة، والإفصاح عن المعلومات، ومسؤولية الوسيط غير المباشر. كما إن هناك العديد من التوصيات لتغييرات السياسة لتحسين الأمن السيبراني من مثل التخفيف من إصابات البرامج الضارة عبر مزودي خدمة الإنترنت من خلال التنظيف المدعوم، والكشف الإلزامي عن خسائر الاحتيال والحوادث الأمنية، والكشف الإلزامي عن حوادث نظام التحكم والتطفل، وتجميع تقارير التجسس الإلكتروني وتقديمها إلى منظمة التجارة العالمية (Moore, 2010: 103).

تمثل المخاطر السيبرانية أحد مصادر الخطر المهمة بالنسبة للمصارف والشركات، وإن من أهم مخاطر التشغيل في المصارف والكثير من المؤسسات هي المخاطر السيبرانية وأمن البيانات، وعلى الرغم من عدم وجود توافق في الآراء حول تعريف دقيق للمخاطر السيبرانية فإنها توصف بأنها قدرات على تعطيل الخدمات الأساسية أو تهديد تقديمها، أو استغلال نقاط الضعف لسرقة المعلومات والأموال من قبل الجهات الفاعلة السيبرانية والبلدان"، ويعرفها معهد إدارة المخاطر بأنها أي خطر يتعلق بحدوث خسائر مالية أو تعطيل أو ضرر لسمعة المؤسسة نتيجة تعطل أحد أنظمة تكنولوجيا المعلومات الخاصة بها (Kamiya et al., 2018:3).

ووفقاً لما تقدم يتبين أن تزايد الهجمات الإلكترونية الرقمية قاد إلى جعل الأمن السيبراني أولوية للمصارف والأفراد، فبالنسبة للمصارف يمكن أن تؤدي الجرائم الإلكترونية إلى خسائر مالية، وتعطل العمليات، واختراق البيانات، وفقدان الثقة في هذه المصارف، بينما يواجه الأفراد سرقة الهوية، والاحتيال المالي، وانتهاك الخصوصية (الباحثة).

ب. مفهوم المخاطر المالية: عرفت المخاطر بانها احتمال وقوع الخسارة، ووفقا لذلك فأن احتمالية حدوثها هي العنصر الأساس فهي ليست مؤكدة او ليست مستحيلة، إذ تنشأ تلك المخاطر من خلال انشطة مختلفة لها طبيعة مالية من مثل المبيعات والمشتريات والاستثمارات والقروض وأنشطة مختلفة أخرى (السويدي، 2011: 152).

إن وجود الخطر في المؤسسات هو شر لا بد منه ولا يمكن تجاهله، لذا كان لزاماً على القائمين على إدارة المؤسسات بعامة والمؤسسات المالية بخاصة إدارة هذه المخاطر بشكل مناسب بهدف السيطرة عليها، لهذا فقد تم انشاء إدارة متخصصة في هذه المؤسسات تدعى بإدارة المخاطر، وإن ادارة المخاطر لا تعني التخلص منها وذلك لأن التخلص من المخاطر يعني في الوقت نفسه التخلص من العائد المتوقع، أما ادارة المخاطر فهي تعني استخدام الأدوات المناسبة لتقليل الخسائر المحتملة والسيطرة قدر المستطاع على هذه المخاطر. تعرف إدارة المخاطر بأنها عبارة عن إجراءات مخطط لها من أجل تحديد الاستجابة وتحليلها ومتابعة المخاطر المتعلقة بأي مؤسسة تتضمن الاجراءات والأدوات والتقنيات التي ستساعد مدير المؤسسة على تعظيم إمكانية وأسباب تحقيق نتائج ايجابية وتخفيض إمكانية وأسباب تحقيق نتائج غير ملائمة (محمد، 2023: 293).

كما تم تعريف المخاطر المالية على أنها مواقف يسودها حال من عدم اليقين المرتبطة بأي شكل من أشكال التمويل، بما في ذلك مخاطر الائتمان، ومخاطر الأعمال، ومخاطر الاستثمار، ومخاطر التشغيل (Peng et al, 2011: 2906). ولقد أصبحت المخاطر المالية أكثر بروزاً وأهمية في تصفية الشركات منذ الانهيار المالي والاقتصادي العالمي عام 2007، إذ ترتبط المخاطر ارتباطاً وثيقاً بجوهر المؤسسة المالية، فهي تنشأ من خلال مجموعة واسعة من المعاملات ذات الطابع المالي بما في ذلك البيع والشراء، والاستثمارات والقروض ومختلف الأنشطة التجارية الأخرى، كما يمكن أن تنشأ هذه المخاطر نتيجة للمعاملات القانونية والمشاريع الجديدة وعمليات الدمج والاستحواذ وتمويل الديون، أو من خلال أنشطة الإدارة، أو أصحاب المصالح الأجنبية، أو المنافسين، أو الحكومات (عيساوي ومرغاد، 2014، 152).

كذلك تم تعريف المخاطر المالية بأنها المدى الذي قد يتعرض فيه المصرف لخسائر أو أحداث غير متوقعة أو غير مخطط لها، التي تنعكس على المؤشرات المالية للمصرف (الموسوي والخفاجي،

2020: 12). كما عرفت بأنها احتمالية وقوع وضع غير مرغوب فيه وخسارة للبنك، وتتجلى المخاطر المالية في التمويل الذي يزيد بشكل كبير من احتمالية الاعتماد على الديون (طعيس، 2023، 123).

تتعلق المخاطر المالية بقابلية الوحدة الاقتصادية بالوفاء بالتزاماتها المالية طويلة وقصيرة الأجل اتجاه الاخرين وكذلك لتمويل فرصها المربحة، فقد تكون الوحدة الاقتصادية غير قادرة على الايفاء بالتزاماتها اتجاه الغير وهنا يؤشر وجود خطورة مالية. وكلما كان معدل السيولة منخفضاً في الوحدة الاقتصادية سيؤدي ذلك إلى ارتفاع درجة المخاطر المالية فيها (الحسنكو، 2004، 47). اما ادارة المخاطر المالية فهي تعرف بأنها "تلك العملية التي يتم من خلالها مواجهة المخاطر وتحديدها، وقياسها ومراقبتها، والرقابة عليها، وذلك لضمان فهم كامل لها (Donald et al, 2013: 20).

تؤثر المخاطر المالية في مخاطر السوق ومخاطر الائتمان ومخاطر التشغيل وتتأثر بها أيضاً، وذلك بسبب وجود علاقة ترابط فيما بينها، إذ يذهب البعض من المحللين إلى القول إن مخاطر السوق والائتمان والتشغيل هي فروع من المخاطر المالية، فمخاطر السوق هي المخاطر التي تنشأ عنها الخسائر بسبب تقلبات أسعار السوق، أما مخاطر الائتمان فهي تلك الخسائر الناتجة عن أن الأطراف المقابلة التي ربما تكون غير راغبة بالوفاء بالتزاماتها التعاقدية أو غير قادرة عليه، أما مخاطر التشغيل فهي تلك المخاطر التي تمثل الخسارة الناتجة عن الفشل أو عدم كفاية العمليات الداخلية والأنظمة والأشخاص أو من أحداث خارجية (Jorion, 2011: 284).

ووفقاً للتعريفات السابقة فإنه بالإمكان تعريف المخاطر المالية بأنها احتمال تعرض المصارف لخسائر ونتائج غير متوقعة نتيجة التمويل الممنوح للغير، وهي على أنواع عدة (الباحثة).

ج. مراحل المخاطر المالية: تمر المخاطر المالية بمراحل عدة، منها (عبود وجاسم، 2020: 189):

المرحلة الأولى هي ظهور حدث كارثي، إذ تواجه المصارف حدثًا ماليًا كارثيًا، من مثل التزام مالي كبير يُثقل كاهل ميزانيتها العمومية دون أن تُدرك ذلك.

المرحلة الثانية هي مرحلة تجاهل ما حصل من أحداث سابقة، إذ إن الإدارة تتجاهل ما يحيط بها من المخاطر نتيجة الحدث الكارثي الذي ظهر في المرحلة السابقة.

المرحلة الثالثة: هي المرحلة التي يزداد فيها الخطر مع استمرار تجاهل الإدارة، وتُسمى (مرحلة التعايش مع الوضع الراهن)، وهنا تبدأ الخسائر بالتراكم على الإدارة.

المرحلة الرابعة: هي مرحلة التعايش مع التعثر المالي، إذ تصبح هذه العملية طبيعية، وتؤثر بدورها في توقف الالتزامات، وبدء الدائنين بالمطالبة بحقوقهم.

في المرحلة الخامسة، بناءً على محفظة المخاطر المالية، فأنه يتم تحديد مجالات أكثر أنواع النشاط المالي للمصارف خطورة وفقًا لمعيار اتساع المخاطر الناتجة (Svetlana et al., 2017: 514).

المبحث الثاني: تأثير الأمن السيبراني في إدارة المخاطر المالية والمصرفية

شهد القطاع المصرفي في السنوات الأخيرة ارتفاعاً غير مسبوق في تهديدات الأمن السيبراني، تزامناً مع الرقمنة السريعة وزيادة المعاملات المالية عبر الإنترنت، إذ تشير الإحصاءات الأخيرة الصادرة عن صندوق النقد الدولي إلى ارتفاع كبير في التهديدات السيبرانية، لا سيما منذ جائحة كوفيد-19، إذ تضاعفت الهجمات الإلكترونية بأكثر من الضعف، ويُعد القطاع المالي معرضاً للخطر بشكل خاص نظراً لتعامله مع البيانات الحساسة، إذ تمثل الهجمات على المؤسسات المالية ما يقرب من 20% من جميع الحوادث. لقد تضاعف التأثير المالي للحوادث السيبرانية الشديدة أربع مرات منذ عام 2017 ليصل إلى 2.5 مليار دولار، فضلا عن التكاليف غير المباشرة من مثل الضرر

الذي يلحق بالسمعة وترقيات الأمن المكلفة، فضلا عن ذلك فقد شهدت المصارف الأمريكية الأصغر حجمًا تدفقات ودائع متواضعة، ولكنها كانت مستمرة في أعقاب الهجمات الإلكترونية، مما أثار مخاوف بشأن الآثار النظامية المحتملة على الاستقرار المالي، وقد أثار هذا التوجه مخاوف كبيرة بشأن تأثير مخاطر الأمن السيبراني في سلوك المصارف وبخاصةً فيما يتعلق بتحمل المخاطر (Sulong et al., 2025: 1-2).

ومع تزايد وتيرة الهجمات الإلكترونية واختراقات بيانات الأمن السيبراني نتيجةً للتطورات التكنولوجية الكبرى، تتزايد دعوات الجهات المعنية إلى إفصاح أكثر شفافية من جانب المؤسسات بشأن المخاطر الإلكترونية التي تواجهها، وكيفية تحديدها وقياسها، والاستراتيجيات والإجراءات التي تتخذها لإدارة هذه المخاطر. وبناءً على ذلك فقد وجّهت الجهات التنظيمية المالية وواضعو معايير المحاسبة اهتمامهم في الوقت الحاضر نحو الإفصاح عن المخاطر الإلكترونية والأمن السيبراني كجزء من افصاحات مخاطر الأعمال، ولقد أصدرت الجهات التنظيمية في الولايات المتحدة الأمريكية وكندا العديد من الإرشادات التي تُسلّط الضوء على أهمية الإفصاح عن الأمن السيبراني، ومع التزايد المستمر في مخاطر الهجمات الإلكترونية، إذ إن هيئة الأوراق المالية والبورصات الأمريكية قامت بإصدار تعليمات تطلب من الجهات المسجلة فيها تقديم افصاحات موحدة ومُحسّنة حول ما أصابها من حوادث إلكترونية، وكذلك تقديم افصاح بشأن الأمن السيبراني وإدارة المخاطر الإلكترونية والاستراتيجية والحوكمة والحوادث (Elsayed et al., 2024: 2).

أ. **خطوات الإدارة الفعالة لمخاطر الأمن السيبراني:** إن الغرض العام من إدارة المخاطر هو تقييم الخسائر المستقبلية المحتملة للمصارف واتخاذ تدابير تعويضية لمعالجة هذه المشاكل المحتملة عند حدوثها، إذ تعمل إدارة المخاطر على تشخيص المخاطر التي قد تواجهها المصارف ومعالجتها، وتعظيم القيمة المتوقعة لجميع أنشطة المصارف وتوجيه الموظفين لفهم العوامل البيئية المحتملة التي تؤثر في أعمال المصرف (بغدادي، 2017: 11). بينما يعتقد البعض أن إدارة مخاطر الامتثال من قبل المصارف تتم عبر مراحل عدة، تشمل تحديد المخاطر وقياسها ومراقبتها، وأخيرًا السيطرة عليها والتخفيف منها (Dniestrzanska, 2015, 167)، لكن مع ذلك، يعتقد البعض أنه يمكن تلخيص عملية إدارة المخاطر في الخطوات الثلاث الآتية (الموسوي والخفاجي، 2023: 167):

- ❖ تحديد وتقييم المخاطر المحتملة في العمل المصرفي.
- ❖ وضع وتنفيذ خطة عمل للتعامل مع وإدارة هذه الأنشطة التي قد تترتب عليها خسائر محتملة.
- ❖ مراجعة ممارسات إدارة المخاطر والإبلاغ عنها باستمرار بعد تطبيقها.

هناك عدد من خطوات الإدارة الفعالة المتعلقة بمخاطر الأمن السيبراني تتلخص فيما يأتي (Eaton, 2019: 3):

1. تحديد أولويات ومخاطر التعرض للأمن السيبراني بالاستعانة بالخبرات في تكنولوجيا المعلومات وتهديدات الأمن السيبراني الحالية.
2. تصميم نظام رقابة وضوابط الأمن السيبراني ونظام رقابة تكنولوجيا المعلومات للتعامل مع المخاطر المحددة في المرحلة الأولى في ضوء أفضل ممارسات الصناعة الحالية ومعايير الرقابة (من مثل معايير رقابة الأمن السيبراني للمعهد الأمريكي للمحاسبين القانونيين).

3. اختبار الفعالية التشغيلية لعناصر رقابة الأمن السيبراني من خلال اختبار ضوابط تكنولوجية سواء أكان ذلك في أثناء مراجعة القوائم المالية أم من خلال الخدمات الاستشارية في مجال تكنولوجيا المعلومات أو المراجعة الداخلية.
4. إعداد تقارير خارجية عن الأمن السيبراني وذلك وفقاً لمعايير خارجية من مثل إطار تقرير المنشأة عن الامن السيبراني للمعهد الأمريكي للمحاسبين القانونيين.
5. الحصول على خدمات التأكيد من شركات المراجعة بخصوص فعالية برنامج إدارة مخاطر الأمن السيبراني للشركة الذي يتوقف على نجاح المراحل الأربع السابقة ويمكن إصدار تقارير خاصة بفعالية برامج إدارة مخاطر الأمن السيبراني للشركة من دون إعلانه للأطراف الخارجية. أما إذا تم إعلانه خارجياً فلا يمكن لشركة المراجعة تقديم أية خدمات استشارية في المراحل الأربع السابقة لضمان استقلال المراجع الخارجي.

ب. تأثير الأمن السيبراني في إدارة المخاطر المالية والمصرفية: عند الحديث عن تأثير الأمن السيبراني في إدارة المخاطر المالية والمصرفية نجد إن دوره يكمن في:

1. **الحد من الخسائر المالية:** جلبت رقمنة القطاع المالي فوائد جمة من حيث الكفاءة وسهولة الوصول وقابلية التوسع، لكن مع ذلك فقد وسّع هذا التحول أيضًا نطاق هجمات مجرمي الإنترنت، مما جعل المصارف والمؤسسات المالية أكثر عرضة لمجموعة واسعة من تهديدات الأمن السيبراني، وذلك من خلال الخدمات المصرفية عبر الإنترنت والمعاملات عبر الهاتف المحمول إلى منصات التكنولوجيا المالية والعملات الرقمية، يعتمد المشهد المالي الآن بشكل كبير على التقنيات المترابطة والعمليات القائمة على البيانات، وبينما مكنت هذه التطورات من الابتكار، إلا أنها طرحت أيضاً تحديات أمنية سيبرانية معقدة تهدد سرية البيانات والخدمات المالية وسلامتها وتوافرها، وإن الهجمات السيبرانية المتمثلة ببرامج طلب الفدية أو اختراق بيانات العملاء قد تكلف المصارف والمؤسسات المالية مبالغ طائلة، لذلك فأن وجود أنظمة أمنية قوية يقلل من تكرار حدوث هذه الحوادث وتقيل حدتها، هذا فضلا عن تقليل الخسائر المالية أو الحد منها (Ibrahim, 2025: 1-2).
2. **تحسين تصنيف المخاطر:** يُعد الأمن السيبراني اليوم واحدا من المكونات الأساسية في تقييم المخاطر المؤسسية، إذ إنه كلما كانت البنية السيبرانية أكثر قوة، كان التقييم الائتماني والاستثماري أكثر إيجابية، ويؤدي تقييم الأمن السيبراني إلى تحديد وتطبيق تدابير أمنية لحماية البيانات المالية والحساسة المخزنة في النظام. وهذا يُسهم في الحد من مخاطر الاختراق وتسريب البيانات المالية، مما قد يُسبب خسائر مالية كبيرة ويؤثر سلبًا في سمعة الكيان الاقتصادي. كما إن تقييم الأمن السيبراني يتيح للوحدات الاقتصادية فرصة للامتثال للتشريعات واللوائح المتعلقة بحماية بيانات هذه الكيانات الاقتصادية وخصوصيتها، وتعزيز ثقة الزبائن وموثوقيتهم بهذه الكيانات وذلك من خلال تدابير أمنية قوية تعزز أنظمة المحاسبة والموثوقية الخاصة بها، ومن ثم تعزيز ثقة العملاء والشركاء التجاريين والمستثمرين، والحد من الاضطراب التشغيلي من خلال التخفيف من مخاطر الهجمات والاختراقات الإلكترونية. كما أن تقييم متطلبات الأمن السيبراني يمكن أن يحافظ على استمرارية الأعمال، ويقلل من خسائر الإنتاجية والتكاليف، ومن ثم يعزز استدامة الوحدات الاقتصادية واستقرارها من خلال توفير بيئة محاسبية آمنة وموثوقة تساهم في تحقيق أهدافها المالية والتشغيلية بشكل فعال (Maryoush and Wathiq, 2024: 524).

3. **الامتثال للأنظمة والتشريعات:** يلعب الامتثال الأمني دوراً حاسماً في تشكيل وضع الأمن السيبراني وتعزيزه للمؤسسات، ويشمل ذلك الالتزام بالمعايير القانونية والتنظيمية ومعايير القطاع التي تحكم حماية البيانات والخصوصية وتدابير الأمن، إذ إن اللوائح الرئيسة من مثل اللائحة العامة لحماية البيانات (GDPR) وقانون نقل التأمين الصحي والمساءلة (HIPAA) وأمن بيانات صناعة بطاقات الدفع (PCI DSS)، إلى جانب المعايير الدولية من مثل ISO/IEC 27001 وNIST، تُلزم المؤسسات بتطبيق أطر أمنية تهدف إلى إدارة المخاطر وحماية البيانات الحساسة وضمان سرية المعلومات وسلامتها وتوافرها، ويتجاوز تأثير الامتثال الأمني مجرد الالتزام التنظيمي، فمن خلال تطبيق أطر الامتثال تُعزز المؤسسات قدرتها على التخفيف من حدة التهديدات والاستجابة للحوادث والتعافي من الخروقات الأمنية بشكل أكثر فعالية. إذ تساعد هذه الأطر على ضمان اتساق تدابير الأمن وتوثيقها جيداً ومواءمتها مع أفضل ممارسات القطاع، فضلا عن ذلك يُعزز الامتثال المساءلة التنظيمية من خلال اشتراط إشراف الإدارة وتعزيز ثقافة تُولي الأمن الأولوية على جميع المستويات. لكن مع ذلك، يُمثل الامتثال أيضاً تحديات لأنه يوجب على المؤسسات الموازنة بين عملية الحفاظ على الامتثال التي غالباً ما تتطلب موارد كثيفة، والحاجة إلى استراتيجية أمنية استباقية تُعالج التهديدات السيبرانية الناشئة. كما يُنظر إلى الامتثال أحياناً على أنه نشاط "مُجرد تحقق"، مما قد يؤدي إلى فجوة بين الالتزام باللوائح التنظيمية والاحتياجات الأمنية الفعلية. فضلاً عن ذلك، يتطلب مشهد التهديدات المتطور باستمرار تحديثات مستمرة لأطر الامتثال، وهو أمر قد يكون مُكلفاً ومعقداً وبخاصةً بالنسبة للمؤسسات متعددة الجنسيات التي تعمل في ظل أنظمة تنظيمية مختلفة، يمكن أن يؤدي عدم الامتثال إلى عواقب وخيمة بما في ذلك العقوبات القانونية والخسائر المالية والإضرار بالسمعة وانقطاعات التشغيل، ومع تطور التكنولوجيا والتهديدات السيبرانية فإنه ستزداد أهمية العلاقة بين الامتثال الأمني والأمن السيبراني، مع تركيز أكبر على دمج النُهج القائمة على المخاطر والأتمتة في إدارة الامتثال (Folorunso et al, 2024: 2015).

4. **تعزيز ثقة العملاء:** في ظلّ المشهد الرقميّ المعاصر فأن الأمن السيبرانيّ لم يعد مجرد ضرورة تقنيّة فحسب، بل عاملاً حاسماً في تعزيز ثقة العملاء، ومع تزايد حوادث اختراق البيانات والهجمات السيبرانية فإنه يجب على المؤسسات إعطاء الأولوية لتدابير أمن سيبرانيّ فعّالة للحفاظ على ثقة العملاء، ولا شك أن دور الأمن السيبراني في تعزيز ثقة العملاء هو أمر بالغ الأهمية، ففي عصر تتزايد فيه انتهاكات البيانات فإنه يجب على المؤسسات إعطاء الأولوية للأمن السيبراني ليس فحسب كإجراء تقني، بل كضرورة استراتيجية للحفاظ على الثقة، ويوافر علم البيانات أدواتٍ ورؤىً قيّمة تُحسّن بروتوكولات الأمن وتُعزز علاقات العملاء. بالاستثمار في تدابير أمن سيبراني فعّالة وتوظيف استراتيجيات قائمة على البيانات، يُمكن للشركات بناء علامة تجارية موثوقة وضمان نجاحها على المدى الطويل (Alwabel, 2024: 1-5).

5. **التكامل مع نماذج إدارة المخاطر:** يُمثل دمج إدارة مخاطر الأمن السيبراني ضمن نطاق الإدارة الاستراتيجية نقلة نوعية تُقرّ بالصلة الوثيقة بين المرونة الرقمية واستراتيجية المؤسسة، ومن خلال دمج اعتبارات مخاطر الأمن السيبراني في عمليات صنع القرار الاستراتيجي، تتبنى المؤسسات موقفاً استباقياً ضد التهديدات السيبرانية المتطورة، ومواءمة التدابير الوقائية مع الأهداف التجارية الشاملة. يُمكّن هذا التكامل التكافلي المؤسسات ليس من تعزيز بنيتها التحتية الرقمية فحسب، بل أيضاً من الاستفادة من مبادراتها الاستراتيجية لتعزيز المرونة السيبرانية، وغرس نهج متماسك يحمي

الأصول، ويضمن استمرارية الأعمال، ويحافظ على ثقة أصحاب المصلحة في بيئة رقمية متزايدة. إن دمج إدارة مخاطر الأمن السيبراني ضمن إطار استراتيجي ليس مجرد ممارسة تقنية فحسب بل هو ضرورة استراتيجية، فالتكامل الفعال يُعزز الأصول الرقمية ويحمي المبادرات الاستراتيجية، ويعزز مرونة المؤسسات في مواجهة التهديدات السيبرانية، ومن خلال تبني نهج شامل يُدمج إدارة المخاطر في جميع جوانب التخطيط الاستراتيجي ترتقي المؤسسات بالأمن السيبراني من مجرد اعتبار تقني إلى عنصر أساسي في عملية صنع القرار الاستراتيجي (Mizrak, 2023: 99).

ج. **إدارة المخاطر المالية:** تتناول إدارة المخاطر المالية العلاقة بين العائد المطلوب وبين المخاطر التي تصاحب هذا الاستثمار، وذلك بقصد توظيف هذه العلاقة بما يؤدي إلى تعظيم قيمة ذلك الاستثمار من وجهة نظر المستثمرين، وبالإمكان تعريف المخاطر المالية بأنها استخدام أساليب التحليل المالي وكذلك استخدام الأدوات المالية من أجل السيطرة على مخاطر معينة في الوحدات الاقتصادية والتقليل من آثار هذه المخاطر غير المرغوب فيها، ترتبط المخاطر المالية بما يأتي: مخاطر أسعار الفائدة، ومخاطر أسعار الصرف، ومخاطر السوق، ومخاطر الائتمان، وغيرها، ومع التقدم العلمي والتطور التكنولوجي في ظل العولمة، يواجه المستثمرون العديد من التحديات التي يجب عليهم مواجهتها لتحقيق أقصى قدر من الأرباح، ولن يتحقق هذا دون التحكم في الأخطار المحدقة من حولهم (محمد وآخرون، 2024: 309-310).

تُعدّ المخاطر المالية واحدة من الموضوعات الاقتصادية المهمة التي جرى النقاش فيها مؤخرًا، لا سيما في ظل الأزمة المالية، واليوم، تُعدّ علمًا قائمًا بحد ذاته، يستند إلى علوم الإحصاء والاحتمالات والاقتصاد والمالية، وعلم المخاطر المالية هي مركبات مكونة له فبإدارة المخاطر يدور الحديث حول إمكانية الحد من المخاطر، وذلك نتيجة التقليص من الخسائر المتوقعة عن طريق استراتيجية متبعة في هذا السياق، إذ إن تقليص الخسائر يكون وفقاً لاستراتيجية حكيمة لها القابلية على الاستجابة لسلوك السوق واتجاهاتها، أي بمعنى حدوث بوادر إيجابية لأسواق الأموال (Elyan,2021:14)،

هناك عدد من الأسباب التي دفعت المنظمات للاهتمام بمفهوم المخاطر المالية. ففضلا عن تزايد المنافسة بين المنظمات ورغبتها في الحفاظ على مكانتها، وتسارع وتيرة التغيرات في البيئة الاقتصادية التي أصبحت سمة العصر وعصب الحياة للبيئة بمختلف أنواعها ومسمياتها، كذلك المفاهيم المتنامية للجودة وتكنولوجيا المعلومات والحوكمة والأداء المالي والتشغيلي، والتركيز على تلك المنظمات التي لديها محافظ مالية متنوعة وتدرك كيفية التعامل مع المخاطر المالية التي تتعرض لها أو قد تتعرض لها، وينظر إلى أهمية المخاطر المالية من حيث الاستثمار وقواعد التمويل للمنظمات، بجانب خطط التقاعد والموجودات وكيفية استبدالها، كما تبرز أهمية المخاطر المالية من خلال حساب أدوات التحوط المتاحة وتحسينها، مما يُسهم في خفض تكاليف المؤسسة، ومن ثم فإنها تعمل على تقليل الخسائر وفي مرحلة لاحقة تعمل زيادة الأرباح، وهذا يُزيل الصعوبات المالية ويمنع تراكم الالتزامات الضريبية المتوقعة، مما يُضيف قيمةً للمؤسسة، فضلا عن تعزيز حقوق المساهمين فيها (Bartram, 2016: 56).

تلعب التكنولوجيا دوراً حاسماً في مختلف مجالات حياتنا، وبخاصةً في القطاع المصرفي، إذ عززت التكنولوجيا القطاع المصرفي ومؤسسات الخدمات المالية بشكل فعال، لقد أحدث التطور التكنولوجي المتسارع والمذهل تحولاً جذرياً في آلية عمل القطاع المصرفي حول العالم، مما أتاح

العديد من الفرص للمؤسسات المصرفية لتحسين مستوى الخدمات المقدمة للعملاء، وتطوير مستواها في الوقت نفسه، وفي الوقت الراهن مكنت التكنولوجيا المصارف ومؤسسات الخدمات المالية من تقديم الخدمات المصرفية والمالية من خلال المعاملات الإلكترونية، مما يوفر الوقت والجهد والمال اللازمين (Shehab et al, 2024: 168).

على الرغم من الفرص والإمكانيات التي تتيحها التكنولوجيا في القطاع المصرفي، إلا أنها تُمثل أيضاً تحدياً خاصاً للقطاع المصرفي نفسه ومؤسسات الخدمات المالية، وندرك جميعاً أن الاستخدام الخبيث للتكنولوجيا يؤدي إلى تعطيل البنية التحتية للمصارف ومؤسسات الخدمات المالية، وخرق الأمن، وزعزعة ثقة العملاء، وتعريض الاستقرار المالي للخطر، وغيرها من الجرائم الإلكترونية. قد يحدث خرق أمني للمعلومات فجأةً وفي أي وقت، نظراً لترابط كل شيء مع الإنترنت، ويستطيع مجرمو الإنترنت الذين يتلاعبون بإنترنت المصارف ومؤسسات الخدمات المالية اختراق بيانات عملاء المصارف وسرقة أموالهم رقمياً (Tariq, 2018: 1-11).

ومع التطور الكبير في التكنولوجيا في القطاع المصرفي، ازدادت المخاطر المرتبطة بالتكنولوجيا. لذلك، تظهر أنواع وأشكال عديدة من هجمات/تهديدات الأمن السيبراني يومياً فيما يتعلق بالقطاع المصرفي. تُشكل هجمات الأمن السيبراني تهديداً للنظام المالي بأكمله، وهو ما تؤكده التقارير الصادرة في هذا الشأن على المستويات الدولية والإقليمية والمحلية، وفي هذا السياق، تُشير تقارير البنك الدولي إلى تركيز هجمات الأمن السيبراني في القطاع المصرفي ومؤسسات الخدمات المالية، الذي شهد في عام 2016 قفزة كبيرة في هجمات الأمن السيبراني بنسبة 65%، بزيادة قدرها 29% عن العام السابق، كما تشير التقارير المصرفية العالمية إلى أن السرقات ضد القطاع المالي باستخدام البرمجيات الخبيثة زادت بنسبة 80% سنوياً في عام 2015 مقارنة بالعام السابق، في حين شكلت هذه الهجمات 38% من الحوادث المبلغ عنها في عام 2015، ارتفاعاً من 23% في عام 2014 (Camillo, 2017, 196-200).

المبحث الثالث: الجانب العملي

صممت الاستبانة كأداة للقياس، وتضمنت محاور ثلاثة، بالاعتماد على المقياس الخماسي الفئوي التقسيم للعالم ليكرت، وشدة الإجابة المقابلة لكل فئة كما في الجدول الآتي:

جدول (1): شدة إجابات ليكرت

المجال	الموافقة
1.8-1	ضعيفة جداً
2.60-1.81	ضعيفة
3.40-2.61	متوسطة
4.20-3.41	كبيرة
5-4.21	كبيرة جداً

المصدر: (Guillamón, 2022).

بناءً على متوسطات العبارات المحسوبة، تقارن كل منها مع الفئة التي تنتمي لها، والشدة المقابلة لها، ولقد صممت الاستبانة ووزعت على عينة مكونة من 200 من الإداريين والفنيين في مصرف الطيف الاسلامي وعدد من فروعه الذين يمثلون مجتمع الدراسة، ولقد تم تحليل 164 استجابة منها فقط وذلك بعد استبعاد (36) استجابة، إذ إن (15) استمارة لم ترجع إلى الباحثة أصلاً، و (21)

استمارة لم تستوفِ شروط البحث العلمي. كما تم التحقق من الفرضية البحث التي تنص على (يوجد أثر ذو معنوية احصائية لاقتصاديات الامن السيبراني في الحد من المخاطر المصرفية في مصرف الطيف الاسلامي وفروعه العاملة في العراق عند مستوى معنوية 0.05)، فضلا عن الفرضيتين الفرعيتين المنبثقتين منها إذ يتم الاثبات بخطوتين الاولى: من خلال جودة النموذج الخطي في توضيح العلاقات المطلوبة، وذلك باستعمال اختبار (F) والثانية من خلال ايجاد المعادلات الانحدارية التي توضح شكل العلاقة الخطية بين المتغير المستقل اقتصاديات الأمن السيبراني بقسميه (الموارد والامكانيات المادية والعلمية والموارد والامكانيات البشرية) والمتغير المعتمد (الحد من المخاطر المصرفية)، وبعد إجراء التحليل الاحصائي كانت النتائج كما يأتي:

جدول (2) تحليل التباين لانحدار متغير اقتصاديات الامن السيبراني على الحد من المخاطر المصرفية

مصادر التباين	درجات الحرية	مجموع المربعات	متوسط المربعات	قيمة F المحسوبة	مستوى المعنوية
بين المتغيرات	1	58.957	58.957	199.531	0.000
داخل المتغيرات	162	47.867	0.295		
التباين الكلي	163	106.824			

المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS

يوضح الجدول رقم (2) إن قيمة اختبار Fالمحسوبة هي (199.531) وبمقارنتها مع القيمة الجدولية لها التي تستخرج من جداول توزيع F($F_{0.05,\ 1,162}$) والمساوية لـ (3.84) نجد انها اكبر، مما يدل على رفض فرضية العدم التي تنص على عدم جودة النموذج الرياضي الخطي في توضيح العلاقة بين المتغيرين وقبول الفرضية البديلة التي تبين إن النموذج الخطي هو نموذج ملائم لتوضيح العلاقة بين المتغيرين، وعند حساب معاملات الانحدار وتكوين المعادلات الانحدارية نحصل على:

جدول (3): معاملات انحدار متغير اقتصاديات الامن السيبراني على الحد من المخاطر المصرفية

	معامل الانحدار	اختبار t	مستوى المعنوية
ثابت الانحدار	0.761	3.413	0.001
اقتصاديات الامن السيبراني	0.422	14.125	0.000
القيمة الجدولية للاختبار(t0.05, 163)		1.96	

المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS.

تشير النتائج الإحصائية الموضحة في الجدول رقم (3) إلى إن اقتصاديات الأمن السيبراني كان لها تأثيراً معنوياً في الحد من المخاطر المصرفية، وذلك من خلال القيمة المحتسبة لاختبار t (14.125) التي اجتازت القيمة الجدولية لها (1.96)، وهكذا فأن معادلة الانحدار التي توضح هذه العلاقة تأخذ الشكل الآتي:

الحد من المخاطر المصرفية =0.761+0.422 (اقتصاديات الأمن السيبراني)

إن العلاقة الإحصائية الموجبة بين المتغيرين تشير إلى أن تغيراً في اقتصاديات الأمن السيبراني بمقدار وحدة واحدة مع بقاء جميع العوامل الأخرى غير الداخلة في القياس ثابتة سيؤدي إلى تغير مقابل في قيمة الحد من المخاطر المصرفية بمقدار (0.422) وحدة وعند مستوى معنوية 0.05، وهذا الأمر يدل على تحقق فرضية البحث في هذا السياق.

Tikrit Journal of Administrative and Economic Sciences, Vol. 21, No. 72, Part (2): 60-77
Doi: www.doi.org/10.25130/tjaes.21.72.2.4

جدول (4): تحليل التباين لانحدار متغير الموارد والامكانيات المادية والعلمية على الحد من المخاطر المصرفية

مصادر التباين	درجات الحرية	مجموع المربعات	متوسط المربعات	قيمة F المحسوبة	مستوى المعنوية
بين المتغيرات	1	34.567	34.567	77.498	0.000
داخل المتغيرات	162	72.257	0.446		
التباين الكلي	163	106.824			

المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS.

يوضح الجدول رقم (4) أن قيمة اختبار Fالمحسوبة هي (77.498) وبمقارنتها مع القيمة الجدولية لها التي تستخرج من جداول توزيع F($F_{0.05, 1,162}$) المساوية لـ (3.84) نجد إنها أكبر، مما يدل على وجوب رفض الفرضية العدمية القائلة بعدم جودة النموذج الرياضي الخطي في توضيح العلاقة بين المتغيرين وقبول الفرضية البديلة القائلة بأن النموذج الخطي ملائم لتوضيح العلاقة بين المتغيرين، ولقد تم حساب معاملات الانحدار واختبار معنويتها كما يأتي:

جدول (5): معاملات انحدار متغير الموارد والامكانيات المادية والعلمية على الحد من المخاطر المصرفية

	معامل الانحدار	اختبار t	مستوى المعنوية
ثابت الانحدار	1.391	4.910	0.000
الموارد والامكانيات المادية والعلمية	0.666	8.803	0.000

المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS.

يوضح الجدول رقم (5) تقدير قيم معلمات الانحدار مع اختبار معنويتها باستعمال الاختبار t الذي يبين معنويتها العالية، إذ اجتازت قيمة اختبار t المحتسبة القيمة الجدولية لها البالغة (1.96)، وهكذا فإن تقدير معادلة الانحدار التي توضح مقدار تأثير الموارد والامكانيات المادية والعلمية في الحد من المخاطر المصرفية كما يأتي:

الحد من المخاطر المصرفية =1.391+0.666 (الموارد والامكانيات المادية والعلمية)

مما يعني إنه في حال تغير ما في الموارد والامكانيات المادية والعلمية بمقدار وحدة واحدة مع بقاء العوامل الأخرى غير الداخلة في القياس ثابتة سيؤدي إلى تغيير مقابل في قيمة الحد من المخاطر المصرفية بمقدار (0.666) وحدة، وهذا يدل على تحقق فرضية البحث الفرعية الأولى المنبثقة عن فرضية البحث التي تنص على (إن هناك أثر ذو دلالة إحصائية ذات تأثير معنوي للموارد والامكانيات المادية والعلمية المتوفرة في المصرف في الحد من المخاطر المصرفية في مصرف الطيف الاسلامي وفروعه العاملة في العراق عند مستوى معنوية 0.05).

جدول (6): تحليل التباين انحدار متغير الموارد والامكانيات البشرية على الحد من المخاطر المصرفية

مصادر التباين	درجات الحرية	مجموع المربعات	متوسط المربعات	قيمة F المحسوبة	مستوى المعنوية
بين المتغيرات	1	59.281	59.281	201.999	0.000
داخل المتغيرات	162	47.543	0.293		
التباين الكلي	163	106.824			

المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS.

يوضح الجدول رقم (6) أن قيمة اختبار Fالمحتسبة (201.999) كانت أكبر بكثير من القيمة الجدولية لها التي تستخرج من جداول توزيع Fالمساوية لـ (3.84) مما يدل على رفض فرضية العدم والقبول بالفرضية البديلة التي تبين عدم جودة النموذج الرياضي الخطي في توضيح العلاقة بين المتغيرين وقبول الفرضية البديلة القائلة بأن النموذج الخطي هو نموذج ملائم لتوضيح طبيعة العلاقة بين المتغيرين، ولقد تم حساب معلمات الانحدار واختبار معنويتها كما يأتي:

جدول (7): معاملات انحدار متغير الموارد والامكانيات البشرية على الحد من المخاطر المصرفية

	معامل الانحدار	اختبار t	مستوى المعنوية
ثابت الانحدار	1.389	7.804	0.000
الموارد والامكانيات البشرية	0.670	14.213	0.000

المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS.

يوضح الجدول رقم (7) معاملات الانحدار مع اختبار معنويتها باستعمال اختبار t الذي يبين معنويتها العالية، إذ اجتازت قيمتا المختبر الاحصائي t المحسوبتان ($t_{0.05,163}$) القيمة الجدولية لهما البالغة (1.96)، وعليه فإن معادلة الانحدار التي توضح كيفية تأثير الموارد والامكانيات البشرية في الحد من المخاطر المصرفية هي:

الحد من المخاطر المصرفية= 1.389 +0.670(الموارد والامكانيات البشرية)

مما يعني بأن تغيراً في الموارد والامكانيات البشرية والعلمية بمقدار وحدة واحدة بأي مقياس وفق المفهوم المحاسبي مع ثبات العوامل الأخرى سيؤدي إلى حدوث تغير مقابل في قيمة الحد من المخاطر المصرفية وبأي وحدة قياس بمقدار (0.670) وحدة، ويدل ذلك على تحقق فرضية البحث الفرعية الثانية المنبثقة من الفرضية الرئيسة التي تنص على (إنه يوجد أثر ذو دلالة احصائية للموارد والامكانيات البشرية المتوافرة في المصرف في الحد من المخاطر المصرفية في مصرف الطيف الاسلامي وفروعه العاملة في العراق عند مستوى معنوية 0.05)، وتدل النتائج آنفة الذكر على تحقق فرضية البحث والفرضيات الفرعية المنبثقة عنها.

الاستنتاجات والتوصيات

اولاً. الاستنتاجات

1. تم تأكيد فرضية البحث الرئيسة والفرضيتين المشتقتين منها، فقد أشارت نتائج تحليل الانحدار إلى وجود علاقة ذات دلالة إحصائية لمتغير "اقتصاديات الأمن السيبراني" في الحد من المخاطر المصرفية" في المؤسسات المالية والمصرفية لعينة الدراسة.
2. كشف تحليل نتائج تقدير الانحدار عن وجود علاقة ذات دلالة احصائية بين متغيري الموارد والامكانيات المادية والعلمية والموارد والامكانيات البشرية في الحد من المخاطر المصرفية.
3. إن قبول فقرات المتغيرات ونسبة التأييد العالية جداً لها من قِبَل المبحوثين يدعو إلى قبول وتبني جميع الافكار التي طرحتها الباحثة في استبانتها:

أ. اقتصاديات الأمن السيبراني (الموارد والامكانيات المادية والعلمية)

- ❖ البنى التحتية التي يمتلكها المصرف تجعله بعيد المنال عن الهجمات السيبرانية.
- ❖ يمتلك المصرف آلية عمل فعالة تضمن إيصال الخدمة المصرفية بأكثر الطرائق الممكنة أماناً.
- ❖ يتعامل المصرف مع الأجهزة والتقنيات الحديثة المتواجدة فيه بالتحكم فيها من خلال وضع قيود وإجراءات صارمة تجعل من الصعب حدوث الاختراق السيبراني.
- ❖ يستخدم المصرف برنامج جدار حماية فعال موضوع على جميع أجهزة الكمبيوتر الخاصة به

ب. اقتصاديات الامن السيبراني (الموارد والامكانيات البشرية):

- ❖ إن المسؤولين عن صيانة برامج الأمان على الحواسيب الخاصة بالعمل هم اشخاص متخصصون بتكنلوجيا المعلومات.
- ❖ هناك أعداد كبيرة للمتعاملين مع مصرف الطيف الإسلامي وهي مستمرة بالزيادة وذلك بسبب الثقة الكبيرة التي يوليها المصرف بأساليب خدمة للمتعاملين معه وتوفير الخدمة المصرفية بأفضل الطرائق الممكنة.
- ❖ تتمتع إدارة المصرف بمهارات علمية وعملية تستغلها بشكلٍ متميز لخلق بيئة عمل آمنة من المخاطر السيبرانية.
- ❖ يمتلك المصرف نسبة جيدة من الموظفين المختصين لهم معرفة دقيقة بالأخطار الالكترونية وأساليب معالجتها ويعتبرون بمثابة مرجع استشاري موثوق لبقية الموظفين لمساعدتهم في حل مشاكل الهجوم السيبراني.

ج. الحد من المخاطر المصرفية:

- ❖ برامج الحماية التي وضعها المصرف تؤدي دورها بشكلٍ ممتاز في الحد من الهجمات السيبرانية.
- ❖ لدى المصرف طرائقاً استباقية تمكنه من توقع الهجمات السيبرانية وتفاديها قبل حدوثها.
- ❖ تلاقي الدورات التدريبية للموظفين وحملات التوعية والتوضيح للتهديدات السيبرانية التي يعطيها المتخصصون المعرفيون للموظفين دورها في نشر الوعي الأمني الشامل.
- ❖ يؤدي برنامج جدار الحماية الذي يستخدمه المصرف على أجهزة الكمبيوتر الخاصة بها دوره بشكلٍ سليم في التحكم فيما هو مسموح به للمرور عبر المنافذ الالكترونية.
- ❖ تقوم إدارة المصرف بمتابعة الهجمات السيبرانية التي حدثت في العديد من المصارف والمؤسسات الاخرى والاستفادة من تجاربهم في معالجتها.

ثانياً. التوصيات: وفقاً لما تم الوصول إليه من استنتاجات التي أفرزها البحث، فضلاً عن تحليل البيانات فإنه بالإمكان التوصية بما يأتي:

1. يوصي البحث بضرورة اعتماد العلاقات الرياضية الموضِّحَة لتأثير اقتصاديات الأمن السيبراني بقسميه (الموارد والامكانيات المادية والعلمية والموارد والامكانيات البشرية) على الحد من المخاطر المصرفية في المصارف والمؤسسات المالية المستخرجة كوسيلة لتقدير درجة الأمان السيبراني في المصارف والمؤسسات المالية العراقية على المدى القصير، وذلك على أساس أن البيانات والمعلومات هي في تجدد مستمر ومن دون توقف وبدوره فإن التحليل الإحصائي يتجدد معها.
2. ضرورة توفير الاجواء العلمية المناسبة للعمل في بيئة آمنة وذلك من خلال إقامة دورات تثقيفية وتعليمية لكوادر المصارف والمؤسسات المالية للارتقاء بالمستوى المعرفي لهم وجعلهم على استعداد دائم لمواجهة المخاطر.
3. التركيز على وجود خبراء مختصين في مجال الامن السيبراني، والعمل على استقطابهم وتعيينهم في المصارف والمؤسسات المالية، والاستفادة من مهاراتهم وقدراتهم العلمية والمهارية في تحديد المخاطر الداخلية والخارجية المحتملة.
4. ضرورة اعتماد منهاج عمل ثابت ينظم عمليات وضع البرمجيات المهمة للأمن السيبراني وتحديثها دورياً.
5. تطوير برامج تدريب سنوية للمصرف، فضلاً عن تخصيص ميزانيات للأمن السيبراني في اعتماد معايير دولية في هذا السياق.

المصادر

اولاً. المصادر العربية:

1. بغدادي، أنيسة (2017) أثر المخاطر المالية على الأداء المالي في المؤسسة دراسة حالة مطاحن جبل عز الدين بو سعادة، 2013-2015، رسالة ماجستير، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة محمد بوضياف المسيلة.
2. البغدادي، مروة فتحي السيد (2021) اقتصاديات الأمن السيبراني في القطاع المصرفي، مجلة البحوث القانونية والاقتصادية، العدد 76، جمهورية مصر العربية.
3. الحسنكو، رغد رياض عبد الله (2004) تحليل النمو وأثره في المخاطر المالية للأسهم العادية "، رسالة ماجستير، كلية الادارة والاقتصاد، جامعة الموصل، العراق.
4. السويدي، سهام محمد (2011) دراسة تحليلية لمستقبل تطبيق معايير المراجعة الدولية في مهنة المراجعة بالجزائر، الدار الجامعية للطباعة والنشر والتوزيع، الإسكندرية.
5. طعيس، خالد محمد (2023) تأثير المخاطر المالية على ربحية المصارف: دراسة لعينة من المصارف الخاصة الإسلامية في العراق للفترة الممتدة من (2014-2019)، مجلة الريادة للمال والأعمال، جامعة النهرين، المجلد 4، العدد 2.
6. عبود، فرج غني وجاسم، بيداء فاضل (2020) المحاسبة عن المشتقات المالية ودورها في تقليل المخاطر المالية: دراسة تطبيقية في عينة من المصارف العراقية المدرجة في سوق العراق للأوراق المالية، مجلة كلية الإدارة والاقتصاد للدراسات الاقتصادية والإدارية والمالية، المجلد 12، العدد 3.
7. عيساوي، سهام ومرغاد، لخضر (2014) استخدام المشتقات المالية في إدارة المخاطر المالية، أبحاث اقتصادية وإدارية، العدد 15، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة محمد خيضر بسكرة، الجزائر.
8. الفوال، عصام (2020) تقييم إمكانية الاستثمار في تطبيق نظام إدارة أمن المعلومات في قطاع الخدمات والاتصالات السورية، المعهد العالي لإدارة الأعمال، رسالة ماجستير، الجمهورية العربية السورية.
9. محمد، قصي جاسم (2023) العلاقة التكاملية بين الهندسة المالية وإدارة المخاطر المالية، مجلة المستنصرية للدراسات العربية والدولية، الجامعة المستنصرية، المجلد 1، العدد 2.
10. محمد، قصي جاسم وأحمد، ناجي حسن وطه، زياد عز الدين (2024) سياسة ادارة المخاطر المالية في الجهاز الإداري، مجلة وارث العلمية، جامعة وارث الأنبياء كلية الإدارة والاقتصاد المجلد 6، عدد خاص أغسطس.
11. الموسوي، حيدر يونس والخفاجي، آيات حسين (2020) قياس العلاقة السببية للمرونة المالية والمخاطرة المصرفية دراسة مقارنة تطبيقية لعينة من المصارف العراقية والاماراتية، مجلة الإدارة والاقتصاد، المجلد 9، العدد 33.
12. الموسوي، حيدر يونس والخفاجي، آيات حسين (2023) قياس علاقة التأثير والارتباط بين متغيرات المرونة المالية وأثرها في المخاطر المصرفية – دراسة تطبيقية مقارنة لعينة من المصارف العراقية والإماراتية، مجلة أهل البيت 9، العدد 32.

ثانياً. المصادر الأجنبية:

1. Ahokas, J., Kiiski, T., Malmsten, J., & Ojala, L‹M‹(2017) Cybersecurity in ports: a conceptual approach‹In Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment‹Proceedings of the Hamburg International Conference of Logistics (HICL), Vol 2.
2. Alwabel, Rakan Abdullah (2024) The Role of Cyber security in Customer Trust: Data Science Perspectives, World Journal of Advanced Research and Reviews, ResearchGate, No.384188419
3. Camillo, M. (2017). Cybersecurity: Risks and management of risks for globalbanks and financial institutions. Journal of Risk Management in Financial Institutions, Vol.10, No 2.
4. Dniestrzanska, Ewa Losiewicz (2015) Monitoring of compliance risk in the bank, Procedia Economics and Finance, No.26.
5. Donald R. Van Deventer., Kenji Imai and Mark Mesler (2013) Advanced Financial Risk Management", John Wiley & Sons, Second Edition, Singapore.
6. Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and Cybersecurity Risk Management, Current Issues in Auditing, Vol 13, No2.
7. Elsayed, Dalia Hussein., Ismail, Tariq H. and Ahmed, Eman Adel (2024) The impact of Cybersecurity disclosure on banks' performance: the moderating role of corporate governance in the MENA region, Future Business Journal, Vol 10, No 115.
8. Bartram, Söhnke. M (2016) "In Good Times and in Bad: Defined-Benefit Pensions and Corporate Financial Policy, Journal of Corporate Finance, Elsevier, vol. 48(C).
9. Elyan, Salwa (2021) The Role of Financial Risk Management in Achieving Enterprise Profitability, Case Study of the Bank of Agriculture and Rural Development - M'sila -, Master's Thesis, Faculty of Economic, Commercial and Management Sciences, Mohamed Bou Diaf University, M'sila, Algeria.
10. Folorunso, Adebola., Wada, Ifeoluwa., Samuel, Bunmi and Mohammed, Viqaruddin (2024) Security compliance and its implication for Cybersecurity, World Journal of Advanced Research and Reviews, 2024, Vol 24, No (01).
11. Guillamón, María-Dolores (2022) Current Aspects in Business, Economics and Finance Vol. 1, B P International publishing organization.
12. Ibrahim, Abdullah Mohammed (2025) Cybersecurity threats in the financial sector: trends and mitigation strategies, the Seybold Report, ResearchGate, DOI: 10.5281/zenodo, 15387211.
13. Jorion, Philippe (2011) Financial Risk Manager Handbook Plus Test Bank, Global Association of Risk Professionals, Sixth Edition, Wiley Finance.
14. Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2018). What is the impact of successful cyberattacks on target firms? (No. w24409). National Bureau of Economic Research. PwC. 2017. 20th CEO Survey.
15. Maryoush, Sarah Alawi and Wathiq, Ilham Mohamed (2024) Evaluating cyber security requirements for accounting systems in economic units a survey of communication

companies in the local environment, Al-Ghary Journal of Economic and Administrative Scienc Vol. 20 (special issue).

16. Mizrak, Filiz (2023) Integrating cybersecurity risk management into strategic management: a comprehensive literature review, Journal of Business and Management (RJBM),Vol 10, No.3
17. Moore,Tyler(2010) Introducing the Economics of Cybersecurity Principles and Policy Option, Harvard University .
18. Peng, Yi and Wang, Guoxun and Kou, Gang and Shi, Yong, 2011, An empirical study of classification algorithm evaluation for financial risk prediction, Applied Soft Computing, Volume 11, No 2.
19. Shehab, Rami., alismail, Abrar s., Almaiah. Mohammed Amin., Alkhdour, Tayseer., Mahmoud., AlWadi, Belal and Alrawad, Mahmaod (2024) Assessment of Cybersecurity Risks and threats on Banking and Financial Services, Journal of Internet Services and Information Security (JISIS), volume: 14, No 3.
20. Sulong, Zunaidah., Fuszder, Habibur Rahman., Abdullah, Mohammad and Abakah Emmanuel Joel Aikins (2025) Cybersecurity risk and bank risk-taking, Journal of Behavioral and Experimental Finance, Vol.47
21. Svetlana, Pashchenko., Nikolay, Pashchenko and Olga, Krioni (2017) Financial risk management, Advances in Economics, Business and Management Research, volume 38
22. Tariq, N. (2018). Impact of cyberattacks on financial institutions. Journal of Internet Banking and Commerce, Vol.23, No 2.