AL KUT JOURNAL OF ECONOMIC AND ADMINISTRATIVE SCIENCES
Publisher: College of Economics and Management - Wasit University

دور المرونة السيبرانية في تعزيز الثقة الرقمية / دراسة تحليلية لآراء عينة من موظفي البنك المركزي العراقي فرع الموصل

زيد عبد النافع سعيد[1]

الجامعة التقنية الشمالية / الكلية التقنية الادارية /قسم ادارة تقنيات المعلومات

Zaid_abdalnafe@ntu.edu.iq

يزن نافع محمود[2]

جامعة نينوى /رئاسة الجامعة / الموصل / العراق

yazen.nafea@uoninevah.edu.iq

الملخص

تهدف الدراسة إلى التعرف على تأثير المرونة السيبرانية ودورها في خلق الثقافة الرقمية في القطاع المصرفي، لذا تم اعتماد البنك المركزي العراقي/ فرع الموصل لدراسة هذا التأثير، واعتمدت استمارة الاستبانة بوصفها أداة لجمع البيانات؛ اذ وزعت (80) استمارة واسترجعت بشكل كامل وكان الصالح منها للتحليل الاحصائي (73)، وحللت البيانات باستعمال الحزمة الإحصائية للعلوم الاجتماعية (SPSS. V26) من أجل إيجاد التكرارات والنسب المئوية والوسط الحسابي والانحراف المعياري كأدوات لوصف متغيرات البحث فضلا عن استخدام البرنامج الاحصائي (SMART PLS V3) لإيجاد علاقات الارتباط والاثر بين متغيرات البحث واختبار الفرضيات، وقد توصل البحث لعدد من الاستنتاجات كان من أهمها اعتبار المرونة السيبرانية عاملاً حاسمًا في تعزيز مستوى الثقة الرقمية داخل البنك المركزي العراقي/ فرع الموصل، إذ أن العلاقة بين المتغيرين هي علاقة طردية ومعنوية بما يعكس اعتماد مستويات الثقة الرقمية على قدرة المؤسسة في إدارة أبعاد المرونة السيبرانية بصورة فعّالة، وأوصى البحث بضرورة إدراج المرونة السيبرانية ضمن الاستراتيجية العامة للبنك كعنصر من عناصر الحوكمة الرقمية بما يضمن تكاملها مع باقي السياسات الإدارية والتقنية ونشر ثقافة المرونة و الأمن السيبراني بين الموظفين لأجل معرفة اهمية التعامل مع البيانات وحمايتها مما يؤدي إلى تعزيز الثقة الرقمية بينهم وبين المتعاملين معهم، بالإضافة إلى تعزيز التفاعل الإيجابي مع المنصات الرقمية المعتمدة في التعاملات المصرفية.

الكلمات المفتاحية: المرونة السيبرانية، الثقة الرقمية، ابعاد المرونة السيبرانية، الجهات الفاعلة.

Abstract

The study aims at examining the impact of cyber resilience and its role in shaping digital culture within the banking sector. To explore this effect, the Central Bank of Iraq – Mosul Branch was selected as the data of the study. A questionnaire was implemented as the primary data collection tool; 80 questionnaires were distributed and fully retrieved, of which 73 were deemed valid for statistical analysis. Data were analyzed using the Statistical Package for the Social Sciences (SPSS V.26) to obtain frequencies, percentages, means, and standard deviations as descriptive statistics for the study variables. Moreover, the Smart PLS software (V3) was employed to test the hypotheses raised by determining the relationships of correlation and influence between the variables. The study reached to several findings, the most notable of which is that cyber resilience is a critical factor in enhancing the level of digital trust within the Central Bank of Iraq – Mosul Branch. The relationship between the two variables was found to be positive and statistically significant, indicating that levels of digital trust depend on the institution's ability to effectively manage the dimensions of cyber resilience. Based on these findings obtained, the study recommends that cyber resilience be incorporated into the bank's overall strategic plan as a key element of digital governance. This integration would ensure its alignment with other administrative and technical policies; and support the dissemination of a culture of cyber resilience and cyber security among employees. Furthermore, it raises awareness about the importance of data handling and protection that would lead to strengthen digital trust between employees and their clients. Finally, it enhances positive engagement with the digital platforms used in banking transactions

Key words: Cyber resilience, digital trust, dimensions of cyber resilience, actors.

المقدمة

في ظل تنامي الاعتماد المؤسسي على النظم الرقمية وازدياد المخاطر المرتبطة بها، أصبحت المنظمات أكثر عرضة للتهديدات والهجمات السيبرانية التي قد تعرقل أنشطتها أو تهدد استقرارها. في هذا السياق، تبرز المرونة السيبرانية بوصفها قدرة المنظمة على الاستعداد لهذه التحديات، واحتوائها، والتعافي منها بفاعلية، بما يضمن استمرارية العمليات الحيوية دون انقطاع. وتُعد هذه القدرة عاملاً جوهريًا في تعزيز الثقة الرقمية، إذ ترتبط ثقة المستخدمين والمتعاملين بمدى قدرة المنظمة

على الحفاظ على سلاسة الخدمة وموثوقية الأداء في بيئة متقلبة. ومن هنا تنبع أهمية فهم العلاقة بين المرونة السيبرانية والثقة الرقمية، لما لها من دور محوري في دعم الاستقرار المؤسسي وتعزيز الاعتمادية والموثوقية في الفضاء الرقمي.

الفصل الاول: الدراسات السابقة ومنهجية البحث

المبحث الاول: الدراسات السابقة

جدول (1) الدراسات السابقة

ت	الباحث	البحث	الوصف
1	Kjell, Hausken, 2020	Cyber Resilience in Firms , Organizations and Societies, Internet of Things	تشمل المرونة السيبرانية مجموعة متنوعة من الجهات الفاعلة المختلفة، مُصنّفة إلى جهات غير مُهدّدة، وجهات مُهدّدة، وجهات هجينة. تؤثر كل جهة فاعلة بناءً على استراتيجيتها على المرونة السيبرانية التي بدورها تتأثر بها.
2	Chui, K. T., 2023	Building digital trust: Challenges and strategies in cyber security.	تركز على المخاطر السيبرانية وتأثيرها على الثقة الرقمية، لفهم الديناميكيات الدقيقة للثقة الرقمية والتدابير العملية اللازمة لبنائها والحفاظ عليها.
3	Safitra, et.al, 2023	Cyber Resilience: Research Opportunities	يكمن مفتاح النجاح في بناء المرونة السيبرانية هو تكييف التكنولوجيا مع قدرات الموارد البشرية وضمان وجود قيادة قوية في فهم ابتكارات الأمن السيبراني في منع الهجمات السيبرانية.
4	Malik, P. K., 2024	The Role of Digital Trust in Enhancing Cyber Security Resilience	الثقة الرقمية ومرونة الأمن السيبراني ضروريان للاستخدام الآمن والموثوق حيث يساعد في حماية الشبكات والأنظمة والبرامج من الهجمات الخبيثة من خلال استخدام أساليب مختلفة كالتشفير، وإجراء

			عمليات تدقيق أمنية منتظمة.
5	Alhidaifi, et.al, 2024	A survey on cyber resilience: Key strategies, research challenges, and future directions	اصبحت المرونة السيبرانية اساسية في البنية التحتية الحالية لتكنولوجيا المعلومات كونها تشير إلى قدرة المؤسسة على الاستعداد للآثار السلبية الناجمة عن الهجمات السيبرانية التي تؤثر على العمليات التجارية، واستيعابها، والتعافي منها، والتكيف معها.

المصدر: اعداد الباحثين

المبحث الثاني: منهجية البحث

أولا: مشكلة البحث

ان للتطور التكنولوجي الحاصل في وقتنا الحالي تأثيرا كبيرا على طبيعة عمل المنظمات الذي أدى إلى الاعتماد شبه التام على العمل الرقمي وما يصاحبه من خطورة تتمثل بالاختراقات والتهديدات السيبرانية المستمرة التي يكون الغرض منها هو الوصول إلى البيانات الخاصة بالمنظمة ومحاولة تعطيل أنشطتها بما ينعكس سلباً على ثقة العاملين في تلك المنظمات والمستفيدين منها بالتعامل مع أنظمتها الرقمية ومن هنا يبرز دور المرونة السيبرانية في الحفاظ على استمرارية عمل المنظمات اثناء وبعد الهجوم السيبراني والتعافي من اثاره لكون ان أقوى تدابير الامن السيبراني ممكن ان تتعطل بسبب الهجمات المتكررة بشكل يومي لذا تتمثل مشكلة البحث بالتساؤلات الاتية:

1- ما دور المرونة السيبرانية في تعزيز الثقة الرقمية لدى العاملين داخل البنك المركزي؟

2- إلى أي مدى يشعر العاملين ان الاجراءات السيبرانية الحالية كافية لحماية الأنظمة بالشكل الذي يضمن استمرارية الاعمال داخل المنظمة؟

3- هل هناك علاقة ارتباط بين المرونة السيبرانية والثقة الرقمية لدى العاملين داخل المنظمة المبحوثة؟

4- هل هناك تأثير للمرونة السيبرانية على الثقة الرقمية لدى العاملين داخل المنظمة المبحوثة؟

ثانيا: أهمية البحث

تكمن أهمية البحث في مدى مساهمة المرونة السيبرانية في جعل المنظمات قادرة على العمل ضمن بيئة سيبرانية شديدة الخطورة من خلال وضع سياسات استراتيجية شاملة قائمة على التعامل مع المخاطر وليس فقط اتخاذ التدابير الأمنية، كما هو الحال في الامن السيبراني الذي يسعى إلى منع المخاطر والهجمات من الحدوث، ونظرا لمدى حساسية العمل داخل البنك

المركزي وإمكانية حدوث الاختراقات، لذا فان وجود فهم حقيقي لدى العاملين بأهمية الاعتماد على اليات المرونة السيبرانية في القدرة على التعامل مع التهديدات المحتملة وكيفية تجنبها او التكيف معها بالشكل المطلوب ان وقعت وسرعة التعافي منها والعودة السريعة إلى مزاولة الاعمال بشكل طبيعي مما يؤثر على زيادة الثقة الرقمية لدى المتعاملين مع الأنظمة داخل البنك والمتمثلة بجهات داخلية كانت او خارجية.

ثالثا: اهداف البحث

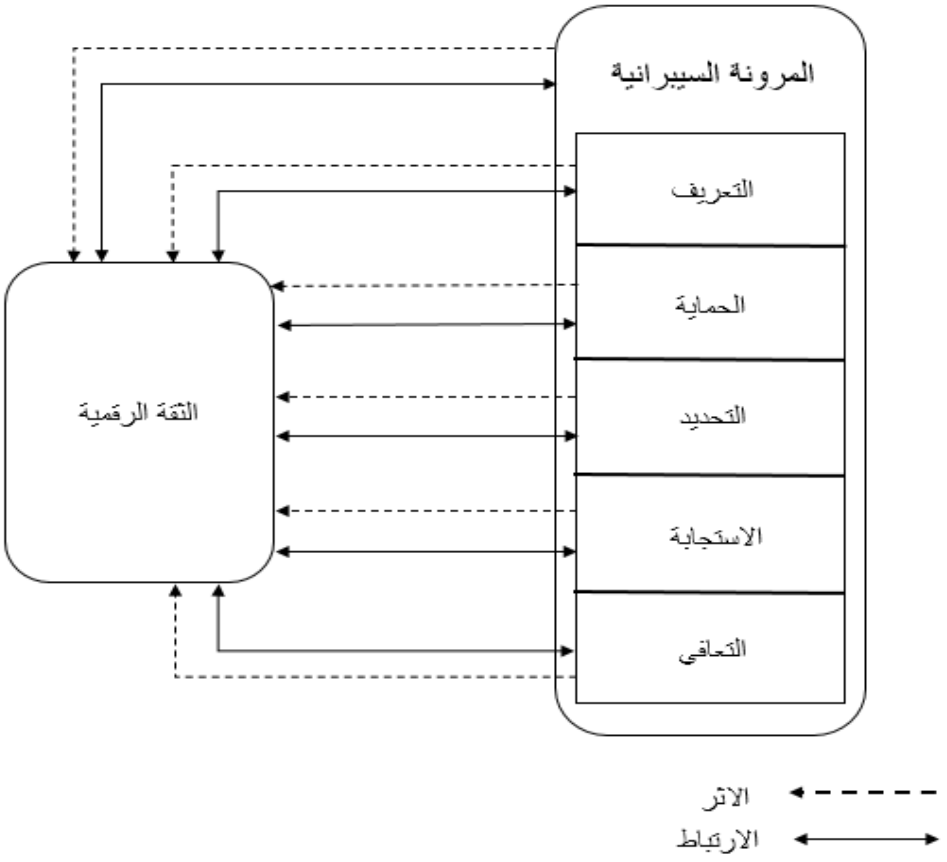
1- تقديم إطار نظري شامل عن المرونة السيبرانية والثقة الرقمية.

2- قياس مدى توافر متطلبات وابعاد المرونة السيبرانية داخل المنظمة المبحوثة.

3- قياس مدى الثقة الرقمية لدى العاملين في المنظمة بأنظمتها الرقمية.

4 - التعرف على طبيعة علاقة الارتباط والاثر بين المرونة السيبرانية والثقة الرقمية داخل البنك المركزي.

رابعا: مخطط البحث الفرضي



الشكل (1) مخطط البحث الافتراضي

المصدر: اعداد الباحثين

خامسا: فرضيات الدراسة

الفرضية الرئيسة الأولى التي تنص على:

((لا توجد علاقة ذات دلالة إحصائية بين المرونة السيبرانية والثقة الرقمية))

وتتفرع منها الفرضية الفرعية الآتية:

((لا توجد علاقة ذات دلالة إحصائية بين أبعاد المرونة السيبرانية والثقة الرقمية))

الفرضية الرئيسة الثانية التي تنص على:

((لا يوجد تأثير ذي دلالة إحصائية للمرونة السيبرانية في الثقة الرقمية))

وتتفرع منها الفرضية الفرعية الآتية:

((لا يوجد تأثير ذي دلالة إحصائية لأبعاد المرونة السيبرانية في الثقة الرقمية))

سادسا: الاساليب وتقنيات جمع وتحليل البيانات

تم اعتماد المنهج الوصفي التحليلي لاختبار الفرضيات وذلك من خلال بيان علاقات الأثر والارتباط بين متغيرات البحث وقياسها بصورة علمية بعد ان تم اعتماد استمارة الاستبانة كأداة بحثية رئيسية التي تضمنت العديد من الأسئلة ذات العلاقة بموضوع البحث، علما ان الاستمارة اعتمدت على مقياس ليكرت الخماسي، وتم الاعتماد في تحليل البيانات الخاصة بالجانب العملي على البرنامج الاحصائي Smart PLS V3 لتحليل نموذج المعادلات الهيكلية باستعمال أسلوب المربعات الجزئية (PLS-SEM) بالإضافة إلى اعتماد الحزمة البرمجية للعلوم الإحصائية (SPSS) لإجراء التحليلات الإحصائية الوصفية المتمثلة بالمتوسطات والانحرافات المعيارية.

سابعا: مجتمع البحث وعينته

تمثل مجتمع البحث بالأفراد العاملين في البنك المركزي العراقي فرع الموصل والبالغ عددهم الكلي (181) موظف وتم توزيع استمارات استبيان بلغ عددها (80) استمارة بوصفه عينة عشوائية واسترجعت بشكل كامل وكان الصالح منها للتحليل الاحصائي (73) استمارة ويوضح الجدول (2) سمات الافراد العاملين في البنك

الجدول (2) سمات الافراد المبحوثين

المتغير	الفئة	العدد	النسبة المئوية %
الجنس	ذكر	35	%47.94
	انثى	38	%52.06
	المجموع	73	%100
المتغير	**الفئة**	**العدد**	**النسبة المئوية %**
العمر	20 – 30 سنة	9	%12.33
	31 – 40 سنة	27	%36.99
	41 – 50 سنة	18	%24.65
	51 سنة – فأكثر	19	%26.03
	المجموع	73	%100
المتغير	**الفئة**	**العدد**	**النسبة المئوية %**
المؤهل العلمي	اعدادية فما دون	3	%4.11
	دبلوم فني	7	%9.59
	بكالوريوس	54	%73.97
	ماجستير	6	%8.22
	دكتوراه	3	%4.11
	المجموع	73	%100
المتغير	**الفئة**	**العدد**	**النسبة المئوية %**
مدة الخدمة	1 – 10 سنة	23	%31.51

الوظيفية	11 – 20 سنة	18	%24.65
	21 – 30 سنة	20	%27.4
	31 سنة – فأكثر	12	%16.44
	المجموع	73	%100

المصدر: اعداد الباحثين

ثامنا: حدود البحث تمثلت حدود البحث بالآتي:

1- الحدود الزمانية: تمثلت بالوقت المستغرق لإنجاز البحث للمدة من (2025/3/20) إلى (2025/9/1).

2- الحدود المكانية: تمثلت بالبنك المركزي العراقي فرع الموصل.

3- الحدود البشرية: شملت عينة عشوائية لعدد من الافراد العاملين في البنك المركزي العراقي فرع الموصل.

الفصل الثاني: المرونة السيبرانية

أولا: مفهوم المرونة السيبرانية وتحديتها

نتيجة للتطور الحاصل في عالم التكنولوجيا والأمن السيبراني اصبحت المرونة السيبرانية مصدر قلق في الاوساط المختلفة بسبب الخروقات المتزايدة وخصوصا في البنية التحتية لتقنية المعلومات (Alhidaifi & others,2024,1). لذلك تحظى المرونة السيبرانية باهتمام كبير من قبل خبراء تكنولوجيا المعلومات بسبب تزايد الهجمات السيبرانية على البيانات والمعلومات (Kott & others,2018,24). حيث تمتلك القدرة على الحفاظ على استمرارية عمل النظام اثناء الهجمات السيبرانية (Asante& others,2021,2) .بالاضافة إلى مقاومة الهجمات والتعافي منها والتكيف معها (Smith,2023,5). وقد عرفها (Keleba & others,2022,) على انها قدرة المنظمة على الصمود والتعافي بسرعة من الهجمات الإلكتروني ، و ذكر (Safitra & others,2023,103) ان هناك تحديات توجه تحقيق المرونة السيبرانية وهي تتمثل بثلاثة نقاط رئيسية وهي **اولا**: **التنظيم** تتمثل المشاكل الرئيسية في انخفاض مستوى الامان الالكتروني بسبب الثغرات والتحديثات الامنية غير الكافية، فضلا عن عدم الفهم الكامل للمستخدمين وقلة خبرتهم، ولتجنب ذلك يجب تعزيز الامان الرقمي وتوفير اطار قانوني، فضلا عن زيادة الشفافية ميزات الامن السيبراني وتمكين الشركات والمستخدمين من استخدام الخدمات الرقمية المتوفرة بأمان عالي . **ثانيا**: **التكنولوجيا** يعد تطوير الانظمة الالكترونية تحول يعتمد على البرامج والتطبيقات المتوفرة والعديدة التي غالبا تكون غير مستمرة ومتداخلة وتبتعد عن الغرض الاساسي الذي تم انشائها من أجله، لذلك يجب معالجة نقاط الضعف في المرونة والامن السيبراني وتحديدا على نطاق صغير لضمان فاعلية الحلول. **ثالثا**: **الموارد البشرية** يعتبر العنصر البشري المحرك الأساسي لتحسين الأمن السيبراني وتعزيز القدرة على مواجهة التهديدات الإلكترونية. كثير من الأحيان، يقوم المستخدمون بنشر بياناتهم الشخصية على الإنترنت دون أن يدركوا المخاطر، مما يُساء فهمه أحيانًا على أنه

خرق أمني. تكمن المشكلة في قلة الوعي والمعرفة بأساسيات الأمن الرقمي بين الأفراد. لذا، يعد نشر الثقافة الأمنية والتدريب المستمر من الخطوات الحيوية لضمان حماية المعلومات وتعزيز السلامة الإلكترونية للجميع لذلك ذكر (others,2024,6 &Renckens) ان هناك مجموعة مخاطر تواجه المرونة السيبرانية بسبب الافراد التي تمثل بالآتي: 1) برامج الفدية: تعد برمجيات الفدية من أخطر التهديدات السيبرانية، إذ تقوم بتشفير بيانات الضحية وطلب فدية مالية مقابل فك التشفير، غالبًا مع تهديدات بنشر البيانات أو حذف النسخ الاحتياطية. لا تقتصر آثار هذه الهجمات على الجوانب التقنية إذ تؤثر بشكل مباشر على استمرارية العمليات التشغيلية للمؤسسات، مما يؤدي إلى توقف الإنتاجية وتكبّد خسائر اقتصادية كبيرة. كما تشمل التداعيات جوانب قانونية وتنظيمية، بالإضافة إلى الإضرار بسمعة المؤسسة وثقة العملاء. 2) الاحتيال عبر البريد الإلكتروني في بيئة الأعمال(BEC) : حيث يقوم المهاجمون، إما باختراق صناديق بريد إلكتروني تابعة للمنظمة المستهدفة، أو بانتحال هوية شخصية موثوقة داخلها. وقد تشمل استخدام برمجيات التحكم عن بُعد أو تسجيل نطاق مشابه لنطاق المنظمة. تؤدي هذه الهجمات إلى تحويل الأموال بشكل غير مشروع، مما يسبب خسائر مالية جسيمة وأضراراً كبيرة على مستوى السمعة المؤسسية. 3) التهديد الداخلي: يشير التهديد الداخلي إلى الأفراد من داخل المؤسسة، ممن يمتلكون صلاحيات وصول مشروعة أو معرفة متقدمة بآلية عملها، ويقومون بإلحاق الضرر بها. وقد يكون هذا الضرر ناتجًا عن اختراق من طرف ثالث (مثل الموردين أو المتعاقدين)، أو نتيجة للإهمال، أو بدافع خبيث. حيث في معظم الحالات، يكون السبب هو قلة الوعي أو الإهمال. 4) اختراق سلاسل التوريد: يعد اختراق سلسلة التوريد أحد أساليب الهجوم السيبراني التي يعتمد فيها المهاجمون على استهداف الموردين أو مزودي الخدمات الخارجيين بدلاً من مهاجمة الجهة المستهدفة بشكل مباشر. ويُستغل هذا النوع من الهجمات بسبب العلاقة القائمة على الثقة والاعتماد بين الأطراف، وخاصة تلك الأقل أماناً، التي غالبًا ما تكون مشاركة في إنتاج أو توزيع أو صيانة البرمجيات والمعدات. في ضوء هذه المخاطر ذكر (World Economic Forum & University of Oxford, 2025,8) إن تحقيق المرونة السيبرانية يحتاج إلى أكثر من إجراء أو أداة معينة، بل إنها تتضمن مزيجًا من الممارسات والجهود التي تصقلها المؤسسة على مر الزمن التي تتكون من سبعة نقاط وهي:

1- القيادة: تمثل في ادارة الاجراءات والجهود الخاصة بالمرونة السيبرانية عن طريق تحديد اهداف معينة ومدى امكانية تحمل المخاطر وتعزيز ثقافة المخاطر والتهديدات الرقمية لدى الافراد.

2- الحوكمة، المخاطر، الامتثال: تعنى بإدارة المخاطر بشكل منتظم، والتبعات القانونية وتحديد الادوار في المنظمة.

3-الموظفون والثقافة: يتم تعزيز ثقافة المرونة السيبرانية من خلال التوعية والتدريب وخلق قوى عاملة تمتلك قدرة الاستباقية والخبرة اللازمة في معالجة التهديدات والخروق الامنية.

4- عمليات الاعمال: تصميم الاليات التي تقدر على الاستمرار وتمتلك المرونة في تقديم الخدمات الحيوية اثناء الاختراقات السيبرانية .

5- الانظمة التقنية: تطبيق وانشاء بنية تحتية تكنولوجية متكاملة لأجل التشغيل والمراقة والتكيف لمنع الحوادث واحتوائها

6- ادارة الازمات: التدرب على ادارة الازمات بشكل يسرع من التعافي بعد الهجمات السيبرانية.

7- مشاركة النظام البيئي: تعزيز التواصل مع الشركاء والموردين في تشارك المعلومات والتهديدات الرقمية لأجل تحديد استراتيجيات لمواجهتها.

ثانيا : الجهات الفاعلة (Actors) في المرونة السيبرانية :

ذكر (Hausken,2020,7) ان المرونة السيبرانية تتمثل بامكانية الجهة الفاعلة على التصدي للحوادث السيبرانية والتعامل معها والتعافي منها لضمان استمرارية عملياتها، حيث ان الجهة الفاعلة تقسم إلى جهة غير مهددة تسعى إلى الحفاظ على المرونة السيبرانية والعمل، الجهة المهددة التي تعرض المرونة السيبرانية إلى الخطر، الجهة الهجينة التي تحافظ على امنها ومرونتها السيبرانية ولكن تعرض امن الشركات الاخرى للخطر.

أ- الجهات المهددة: ذكر (Sailio & Others,2020,7) ان الجهة المهددة تتمثل بثمانية جهات او تهديدات وهي:

1- مجرمي الانترنت: يتسلل هؤلاء إلى الشبكات لأجل استخراج القيمة كالمال او البيانات وتجنب المخالفات القانونية اثناء القيام بذلك، ويقوم مجرمي الإنترنت أيضًا العمل لصالح جهات خارجية أخرى وحتى عمل خدمة لمجرمي الإنترنت الآخرين (Anderson& others,2019,9).

2- الجهات الفاعلة في الدولة القومية: تهدف هذه الجهة إلى جمع المعلومات الضرورية والطلوبة لأجل دعم المصالح الوطنية للبلد.

3- القراصنة والارهابيون: عبارة عن مجموعة من النشطاء يقومون بخرق القوانين وامن الحواسيب للشركات خدمة لقضيتهم او لأجل اثارة الرعب لتحقيق اهداف معينة.

4- باحث عن الاثارة: قد يكون شخص او مجموعة اشخاص يهاجمون انظمة الحواسيب لأجل اثبات الجدارة او التحدي فقط، حيث كان يطلق عليهم سابقا الهاكر ذو القبعة البيضاء، وقد يتسببون في مشاكل غير متوقعة للأنظمة الخاصة بالشركات.

5- التهديد من الداخل: يتمثل بنوعين المرتزق الداخلي الذي قد يستغل حق الوصول إلى البيانات ويبيعها لشركات او جهات اخرى، والنوع الاخر الموظف الساخط الذي يتعرض للطرد او معاملة سيئة داخل الشركة ويسعى للانتقام وإحداث المشاكل.

6- المنافسون: الحصول على معلومات الخصوم كانت وما زالت من الغايات الضرورية لكل مؤسسة خصوصا في المجال التجاري والعسكري، حيث كان التجسس الصناعي وسيلة للوصول إلى المعلومات والمخططات والاسرار التي ينبغي على الشركة المستهدفة حمايتها لأجل الاستثمارات الكبيرة التي تقوم بها بالإضافة إلى حماية الملكية الفكرية

7- الشريك: يتمتع الشركاء بثقة من قبل المتنفذين في الشركة، ويمك ان يكون هذا الشريك عميل، بائع معلومات، موظف سلطات حكومية، ويمكن اساءة استخدام هذه الثقة للوصول إلى شبكة المعلومات المؤمنة، او يمكن ان يعرض الشريك النظام الامني للشركة للخطر عن دون قصد.

8- التسلسل الهرمي للجهات الفاعلة: تستطيع الجهات الفاعلة في اعلى التسلسل الهرمي الاستفادة من الجهات الادنى منها في تحقيق غايتها مثل الحصول على معلومات او مخططات او امكانية وصول لبيانات معينة من خلال التهديد أو بوسائل أخرى (مثل الإكراه أو الخداع أو الرشوة)، وتكون قدوة على اخفاء تورطها بشكل كبير .

ب- الجهات غير المهددة: لا تشكل هذه الجهة اي تهديد، بل تعزز تدابير واجراءات الامن والمرونة السيبرانية وتتمثل هذه الفئة بعدة افراد: 1) فرق الامن السيبراني: الافراد المسؤولون عن حماية النظام والمعلومات والشبكات من التهديدات السيبرانية المختلفة. 2) الهيئات التنظيمية: هي المنظمات التي تقوم بتطبيق المعايير والتعليمات الخاصة بالامن والمرونة السيبرانية. 3) مجموعة التعاون الصناعي: مجموعة افراد او شركات تتشارك التهديدات وأفضل الطرق والتطبيقات لمواجهتها. 4) مزود التكنولوجيا: الشركات التي تقوم بتزويد الادوات والخدمات التكنولوجية لتوفير حلول لمشكلات الامن والمرونة السيبرانية (Verma & others,2025,6)

ت- الجهات الهجينة: عبارة عن اساليب غير تقليدية تستخدم لتحقيق اهداف معينة، وهناك اربعة تحديات في العصر الحديث تجعل من الصعب التعامل مع التهديدات الهجينة وهي: 1) التهديدات المتقدمة تكنولوجيا التي ترعاها الدول. 2) التهديدات السيبرانية المرتبطة بالذكاء الصناعي. 3) استغلال التقنيات الناشئة في التهديد. 4) استغلال نقاط ضعف انظمة سلاسل التوريد، ولغرض التقليل او منع مثل هذه الهجمات، واعتمدت مجموعة اساليب او تدابير معينة لتعزيز التعاون المشترك، واستعمال الذكاء الصناعي في الكشف عن التهديدات، التعلم والاستفادة م المواهب المتوفرة، توحيد السياسات ووضع معايير مشتركة لمواجهة التهديدات (Charter of Trust, 2025, 9).

ثالثا: ابعاد المرونة السيبرانية

ان الفرق الجوهري بين المرونة السيبرانية والامن السيبراني يكمن في كون الأخير يركز على منع الهجمات السيبرانية من الحدوث بينما تركز المرونة على عدم توقف الوظائف والخدمات الأساسية للمنظمات حتى في حالة وقوع الحوادث ومدى قدرتها التعامل مع الهجوم بفعالية والتعافي من اثاره والعودة للعمل بشكل طبيعي بشكل سريع (Shin, 2024, 89294 & Gwanghyun) ووفقا للمعهد الوطني للمعايير والتكنولوجيا (NIST) فقد اعتمد على خمسة وظائف لإدارة المخاطر السيبرانية والسيطرة عليها تتمثل بالتحديد والحماية والكشف والاستجابة والتعافي (Alhidaifi & et.al, 2024, 15) وقد أشار كل من (Gwanghyun & Shin, 2024, 89294) و (Siddiqui, et.al, 2019, 220) و (Carayannis, et.al, 2019, 8) إلى ان المرونة السيبرانية تتكون من الابعاد الآتية:

1- التحديد (Identify): الذي يعني تحسين الفهم التنظيمي من أجل إدارة مخاطر الامن السيبراني بالنسبة للأنظمة والبيانات والأصول داخل المنظمات (Carayannis, et.al, 2019, 8) وتتطلب هذه المرحلة تحليل مكونات الأنظمة ومعرفة تفاعلاتها مع الجهات الداخلية والخارجية لتحديد المخاطر والتهديدات المرتبطة بها ويكون ذلك من خلال نمذجة التهديدات لوصف المهاجم المحتمل واساليبه وأهدافه لاتخاذ التدابير والإجراءات المضادة وبالتالي التقليل من اثار الهجوم او اضعاف دوافع المهاجم من خلال تقليل الفوائد المتوقعة من الهجوم (Siddiqui, et.al, 2019, 220).

2- الحماية (Protect): يتم في هذه المرحلة تطوير وتطبيق إجراءات الحماية المناسبة لضمان تقديم خدمات البنية التحتية الحيوية والقدرة على الحد من تأثير أي هجوم محتمل يصيب تلك البنية واحتواءه (Teodoro, et.al, 2015, 420) وتهدف هذه الوظيفة إلى إدارة الهوية والتحكم في الوصول للمستخدمين والتوعية والتدريب وضمان امن البيانات والمعلومات وصيانة الأنظمة بصورة دورية (Aljumaiah, et.al, 2025, 15) باختصار فان في هذه المرحلة يتم العمل على تطبيق ضوابط امنية تضمن للمنظمات من خلالها استمرارية توافر الخدمات الأساسية لأعمالها حتى مع وقوع الهجمات السيبرانية (Roshanaei, 2021, 95).

3- الكشف (Detect): تطوير وتنفيذ الأنشطة اللازمة والمناسبة لتحديد وكشف وقوع حدث يتعلق بالأمن السيبراني (Ryan & Mclucas, 2015, 7) ويتم في هذه المرحلة التعرف والكشف عن الأنشطة المشبوهة من خلال المراقبة المستمرة لعمل الأنظمة ومقارنتها بالسلوك السليم والامن وبمجرد رصد أي نشاط ضار يتم إصدار التنبيهات للبدء باستراتيجية تخفيف الضرر (Siddiqui, et.al, 2019, 220) اذ يعد الكشف السريع عن الحوادث امراً بالغ الأهمية للمنظمات من أجل تقليل الاضرار من خلال الاستجابة الفعالة والفورية (Costigan & Ni Thuama, 2023, 31).

4- الاستجابة (Respond): عادة ما تدرك المنظمات انه وبالرغم من التدابير الوقائية المتخذة من قبلها للتهيؤ للحوادث السيبرانية الا ان ذلك لا يمنع وقوعها بشكل مطلق مما يجعل الاستجابة لتلك الحوادث بسرعة وفعالية عالية امر بالغ الأهمية للتقليل من الاضرار الناجمة التي تصيب عمل تلك المنظمات (Aljumaiah, et.al, 2025,22) لذا ينبغي على القائمين على العمل بوضع الارشادات الصحيحة والإجراءات المناسبة الواجب اتخاذها عند وقوع الحوادث السيبرانية فضلا عن وجود خطة محكمة ومحددة مسبقا واستراتيجيات اتصال فعالة للتعامل الصحيح مع تلك الحوادث (Costigan & Ni Thuama, 2023, 32).

5- التعافي (Recover): يتم في هذه المرحلة استعادة بيانات النظام وموارده إلى الوضع الطبيعي من خلال إصلاحه وتحديثه وتصحيحه مع وجوب تحديد أسباب وطرق تعطل النظام من خلال جمع الأدلة من النظام المخترق ويتم كل ذلك عن طريق توافر وتنفيذ مهام إدارية بالغة الأهمية والتواصل مع الجهات المعنية لضمان سلامة وامن النظم الحيوية والحفاظ على فاعليتها (Siddiqui, et.al, 2019, 221) كما يتم التركيز في هذه المرحلة على ضرورة التعلم من الحوادث الحالية والسابقة لتحسين إجراءات الامن السيبراني مستقبلاً (Costigan & Ni Thuama, 2023, 32).

الفصل الثالث: الثقة الرقمية

اولاً: المفهوم

يشار إلى الثقة الرقمية على انها ثقة أصحاب المصلحة في قدرة الجهات الفاعلة والتقنيات والعمليات على انشاء وبناء شبكات اعمال موثوقة وامنة (Guo, 2022, 3) فالثقة في العصر الرقمي تعني المفهوم الأساسي الذي يحدد التفاعلات والمعاملات والعلاقات ضمن الفضاء الرقمي الواسع والمترابط، وتعد الثقة أيضا العنصر الأساسي الذي يمكن الافراد من مشاركة المعلومات الشخصية وإدارة الاعمال والتفاعل مع المجتمعات الافتراضية بشكل يضمن السلامة والامن والخصوصية

(CHUI, 2022, 16), وتعد الثقة الرقمية ضرورية جدا لنجاح العمل الجماعي والتعاون وتبادل المعرفة فهي تعمل على تسهيل المفاوضات بين الأطراف وتخفض التكاليف لإنجاز المعاملات بل وتساعد حتى في حل النزاعات السياسية بين الدول (Paliszkiewicz, et.al, 2023, 4), لذا وباختصار فان الثقة الرقمية لا يمكن اعتبارها تقنية او عملية بل هي نتيجة تتجلى في العلاقات الامنة والشفافة والتفاعل بين المنظمات وشركائها وزبائنها ويعتمد تحقيقها على كيفية تأمين البيانات والمعلومات والأصول لجميع المشاركين في اعمال المنظمات ومن ثم، ينعكس ذلك في الحفاظ على سمعة المنظمة ونجاحها في مجال الاعمال في البيئة الرقمية (McClimans, et.al, 2016, 2).

ثانيا: الأهمية

ان انتشار استخدام التكنولوجيا في وقتنا الحالي بشكل كبير جعلها تحتل مكانة متميزة في انجاز المعاملات كافة لذا فقد برز مفهوم مصاحب للتكنولوجيا ينبغي التركيز عليه الا وهو الثقة الرقمية التي تكمن أهميتها في انها تعظم من إمكانيات التقنيات الرقمية التي تمتاز بيئتها بالمخاطر الكبيرة مقارنة ببيئة الاعمال التقليدية مما يجعل الثقة عاملا أساسيا وحاسما في تقليل المخاوف لدى المستفيدين من التقنيات الحديثة بالشكل الذي يحثهم على التفاعل واستخدام التكنولوجيا بشكل كبير وفعال (Saveljeva & Volkova, 2025, 1) وتبرز أهمية الثقة في جعل المستفيدين قادرين على انجاز معاملاتهم وخصوصا المالية منها عبر أنظمة تعتمد الشبكات في عملها بأمان وموثوقية بأن تلك الأنظمة صممت بالشكل الذي يجعلها قادرة على مواجهة التهديدات المحتملة من حين لآخر (Shehzadi, et.al, 2023, 1) وتكمن أهمية الثقة الرقمية بسبب غياب التفاعل المادي في إتمام الاعمال بشكل رقمي الذي قد يعزز من عدم اليقين لدى المستفيدين الذي يقابله عدد من المعتقدات نتيجة توافر الثقة تتمثل بالنزاهة والكفاءة والإحسان وهي جميعها عناصر لابد منها لإنجاز الاعمال بشكل الكتروني (Yacoubian, 2025, 4142) ، فالثقة الرقمية تعد الخيط الخفي الذي لا غنى عنه الذي يربط المستفيدين بالخدمات الرقمية التي يعتمدون عليها في عملهم وهي الأساس الذي تزدهر به الاقتصاديات والديمقراطيات الرقمية سواءً كان ذلك تمكين شركة صغيرة من الوصول إلى عملاء جدد، أم تمكين طالب من حضور دروس افتراضية، أم تمكين مواطن من الوصول إلى خدمات عامة حيوية ويجب أن تكون الثقة حاضرة ليعمل العالم الرقمي بفعالية. إن بناء هذه الثقة والحفاظ عليها ليس مهمة لمرة واحدة بل التزام مستمر، وهو التزام يكمن في انشاء مجتمع رقمي آمن وعادل وجاهز للمستقبل (Bhatnagar, 2025, 2).

ثالثا: التحديات

يتميز المشهد الرقمي اليوم بمجموعة متواصلة ومتطورة من التهديدات السيبرانية التي تؤثر بشكل كبير على الثقة في الفضاء الرقمي، تُشكل الهجمات السيبرانية التي تتراوح من الحملات المتطورة التي ترعاها الدول إلى هجمات برامج الفدية وغيرها تهديدًا مستمرًا لسرية الأنظمة والبيانات الرقمية وسلامتها التي تنعكس سلبا على ثقة المستفيدين والمنظمات في المنصات والخدمات الرقمية لذا ومع هذا الكم الهائل من تلك التهديدات والهجمات يصبح ضروري على محترفي الامن السيبراني اتخاذ التدابير اللازمة كافة لمنعها ومن ثم، بناء الثقة والحفاظ عليها (CHUI, 2022, 16) واليوم اصبح الجميع على معرفة بشأن الاختراقات الأمنية والوصول غير المرخص إلى البيانات الشخصية واستخدامها بشكل غير قانوني مما يجعل الثقة عاملا هش

يمكن ان يتأثر بمثل تلك الاعمال (Szumski, 2020, 3546) وقد حدد (Nafees & Kumar, 2023, 111) تحديات الثقة الرقمية بخروقات البيانات واهتزاز الثقة التي تشمل كل مما يلي:

- إدارة السمعة (تعزيز صورة المنظمة على الإنترنت): من خلال التأثير على كيفية ظهور الأفراد أو المنظمات على الإنترنت بصورة جيدة تضمن الحفاظ على سمعة إيجابية، فعلى سبيل المثال تستجيب المنظمات بفعالية للتغذية العكسية والاخذ بآراء الزبائن ومعالجة شكاويهم عن أمور تتعلق بعملها.
- الاثار طويلة الأمد: ان تكرر الخروقات لأنظمة وبيانات المنظمات ينعكس سلبا على عمل المنظمة بسبب اهتزاز ثقة زبائنها الامر لذا عليها اتخاذ التدابير الأمنية الوقائية للحد من تلك الاثار.

ووفقا لـ (Preecha, 2025, 35) فقد ذكر ان للثقة الرقمية في القطاع الحكومي بعض التحديات تتمثل بما يأتي:

- الثقة في الأنظمة الحكومية: اذ تعد ثقة المواطنين بأنظمة الحكومة لا تزال منخفضة بسبب ضعف التواصل وغياب الوضوح في الإجراءات الحكومية مما جعل الجمهور مترددا في التعامل الكامل مع الخدمات الرقمية.
- تحديات الأمن السيبراني: تُعدّ التهديدات السيبرانية قضيةً حرجةً تؤثر على ثقة المواطنين بالأنظمة الرقمية الحكومية ويرى العديد من المواطنين أن إجراءات الحكومة مثل الوقاية من التهديدات والمراقبة الأمنية المستمرة والاستجابة الفعالة للحوادث غير كافية لمعالجة تلك المخاطر مما يثير الشكوك حول قدرة الحكومة على إدارة التحديات التقنية المعقدة بفعالية.

رابعا: الثقة الرقمية والمرونة السيبرانية

ان تحقيق المرونة السيبرانية يتطلب التزام استراتيجي على مستوى المنظمة ومع زيادة التهديدات السيبرانية أصبح تحقيق المرونة السيبرانية من المتطلبات الاساسية لبناء ثقة رقمية عالية في حماية البيانات والتعاملات التجارية واكتساب ميزة تنافسية (PwC,2024,19). ولقد اشار (Wang & others,2023,6) ان تحقيق الثقة الرقمية يتم من خلال مجموعة قواعد او ادوات تساعد في تحقيق ذلك وتشمل اساليب تحقق قوية لهوية المستخدم كالمصادقة الثنائية او البيومترية للتأكد من وصول المصرح لهم فقط إلى الموجودات الرقمية، بالاضافة إلى عملية التشفير التي تسمح للمستخدم فقط من الوصول، فضلا عن السياسات الامنية المتبعة، حيث تساعد هذه التدابير على حماية الأصول الرقمية من الجهات الخبيثة وضمان الحفاظ على أمان البيانات. ذكر (Malik,2024, 61) ان الثقة الرقمية يمكن الوصول اليها عن طريق تحقيق ما يسمى مرونة الامن السيبراني، التي تقع فيما يسمى بمنطقة الثقة في العالم الرقمي التي تتم من خلال اربعة خطوات هي:

1- تحديد وتقييم المخاطر: يتم تحديد التهديدات المحتملة الحدوث ونقاط الضعف الموجودة وأثرها على المؤسسة.

2- تطبيق الضوابط الامنية: تطبيق التعليمات والتطبيقات والضوابط الادارية والتقنية للتخفيف من المخاطر التي تم تحديدها مسبقا.

3- المراقبة والمراجعة: مراقبة مدى كفاءة وفاعلية الضوابط الامنية ومراجعتها وتحديثها باستمرار وحسب الحاجة.

4- الاستجابة للحوادث: وجود خطة في حالة حدوث خروقات امنية والتأكد من ان المنظمة قادرة على الاستجابة بسرعة وبفاعلية.

الفصل الرابع: الجانب العملي

أولاً: التحليل الوصفي

1- التحليل الوصفي لفقرات لأبعاد متغير المرونة السيبرانية:

تم حساب التكرارات والنسب، فضلا عن المتوسط الحسابي والانحراف المعياري ونسبة الاستجابة لأبعاد متغير (المرونة السيبرانية)، وكما في الجدول أدناه:

جدول (3): وصف وتشخيص فقرات أبعاد المرونة السيبرانية

الفقرات	مقياس الاستجابة										المتوسط الحسابي	الانحراف المعياري	نسبة الاستجابة %
	أتفق بشدة (5)		أتفق (4)		محايد (3)		لا أتفق (2)		لا أتفق بشدة (1)				
	ت	%	ت	%	ت	%	ت	%	ت	%			
X1_1	23	31.9	34	47.2	11	15.3	4	5.6	0	0	4.056	0.837	81.1
X1_2	21	29.2	30	41.7	7	9.7	14	19.4	0	0	3.806	1.07	76.1
X1_3	19	26.4	32	44.4	11	15.3	9	12.5	1	1.4	3.819	1.012	76.4
X1_4	20	27.8	31	43.1	11	15.3	7	9.7	3	4.1	3.806	1.083	76.1
X1_5	17	23.6	28	38.9	12	16.7	8	11.1	7	9.7	3.556	1.243	71.1
التحديد	%27.8		%43.1		%14.4		%11.7		%3.0		3.809	1.049	76.2
	%70.9						%14.7						
X2_1	30	41.1	29	39.7	8	11	4	5.5	2	2.7	4.11	0.994	82.2
X2_2	26	35.6	31	42.5	9	12.3	3	4.1	4	5.5	3.986	1.074	79.7

74.5	1.239	3.726	5.5	4	17.8	13	6.8	5	38.4	28	31.5	23	X2_3
74.0	1.255	3.699	11	8	6.8	5	11	8	43.8	32	27.4	20	X2_4
77.5	1.13	3.877	5.5	4	8.2	6	12.3	9	41.1	30	32.9	24	X2_5
77.6	1.138	3.880	%6.0		%8.5		%10.7		%41.1		%33.7		الحماية
			%14.5						%74.8				
81.9	0.853	4.096	2.7	2	1.4	1	11	8	53.4	39	31.5	23	X3_1
70.7	1.042	3.534	5.5	4	9.6	7	26	19	43.8	32	15.1	11	X3_2
69.9	1.042	3.493	2.7	2	15.1	11	30.1	22	34.3	25	17.8	13	X3_3
73.4	1.094	3.671	4.1	3	15.1	11	11	8	49.3	36	20.5	15	X3_4
77.0	1.287	3.849	11	8	5.5	4	8.2	6	38.3	28	37	27	X3_5
74.6	1.064	3.729	%5.2		%9.3		%17.3		%43.8		%24.4		الكشف
			%14.5						%68.2				
77.8	0.98	3.89	4.1	3	4.1	3	16.5	12	49.3	36	26	19	X4_1
68.8	1.093	3.438	5.5	4	15.1	11	24.6	18	39.7	29	15.1	11	X4_2
70.1	1.056	3.507	4.1	3	12.3	9	30.2	22	35.6	26	17.8	13	X4_3
75.3	0.936	3.767	1.4	1	9.6	7	20.5	15	47.9	35	20.6	15	X4_4
73.4	1.313	3.671	12.3	9	6.8	5	12.3	9	38.4	28	30.2	22	X4_5
73.1	1.076	3.655	%5.5		%9.6		%20.8		%42.2		%21.9		الاستجابة
			%15.1						%64.1				
83.6	0.991	4.178	1.4	1	6.9	5	12.3	9	31.5	23	47.9	35	X5_1

76.7	1.118	3.836	4.1	3	8.2	6	21.9	16	31.5	23	34.3	25	X5_2
77.3	1.018	3.863	4.1	3	6.9	5	13.7	10	49.3	36	26	19	X5_3
78.4	1.115	3.918	5.5	4	6.9	5	12.3	9	41.1	30	34.2	25	X5_4
70.7	1.345	3.534	11	8	16.4	12	8.2	6	37	27	27.4	20	X5_5
77.3	1.117	3.866	%5.2		%9.1		%13.6		%38.1		%34.0		التعافي
			%14.3						%72.1				

المصدر: إعداد الباحثين بالاعتماد على مخرجات برنامج SPSS V26.

يوضح الجدول (3) الخاص بوصف الفقرات لأبعاد المرونة السيبرانية حيث ان المؤشر الكلي للبعد الأول (التحديد) في جانب الاتفاق كان (70.9%) بينما كانت نسبة الافراد المحايدين (14.4%) في حين بلغت نسبة الإجابات للأفراد المبحوثين غير المتفقين (14.7%) ويدعم هذه الإجابات قيمة الوسط الحسابي البالغة (3.809).

اما المؤشر الكلي للبعد الثاني (الحماية) في جانب الاتفاق كان (74.8%) بينما كانت نسبة الافراد المحايدين (10.7%) في حين بلغت نسبة الإجابات للأفراد المبحوثين غير المتفقين (14.5%) ويدعم هذه الإجابات قيمة الوسط الحسابي البالغة (3.88).

في حين كان المؤشر الكلي للبعد الثالث (الكشف) في جانب الاتفاق (68.2%) ونسبة الافراد المحايدين (17.3%) اما عن نسبة الإجابات للأفراد المبحوثين غير المتفقين (14.5%) ويدعم هذه الإجابات قيمة الوسط الحسابي البالغة (3.729).

وبلغ المؤشر الكلي للبعد الرابع (الاستجابة) في جانب الاتفاق (64.1%) بينما بلغت نسبة الافراد المحايدين (20.8%) اما نسبة الإجابات للأفراد غير المتفقين (15.1%) ويدعم هذه الإجابات قيمة الوسط الحسابي البالغة (3.655).

اما المؤشر الكلي للبعد الخامس (التعافي) في جانب الاتفاق كان (72.1%) بينما كانت نسبة الافراد المحايدين (13.6%) في حين بلغت نسبة الإجابات للأفراد المبحوثين غير المتفقين (14.3%) ويدعم هذه الإجابات قيمة الوسط الحسابي البالغة (3.866).

2- التحليل الوصفي لفقرات متغير الثقة الرقمية:

تم حساب التكرارات والنسب بالإضافة إلى المتوسط الحسابي والانحراف المعياري ونسبة الاستجابة لفقرات متغير (الثقة الرقمية)، وكما في الجدول أدناه:

جدول (4): وصف وتشخيص فقرات الثقة الرقمية

الفقرات	مقياس الاستجابة										المتوسط الحسابي	الانحراف المعياري	نسبة الاستجابة %
	أتفق بشدة (5)		أتفق (4)		محايد (3)		لا أتفق (2)		لا أتفق بشدة (1)				
	ت	%	ت	%	ت	%	ت	%	ت	%			
Y_1	29	39.7	28	38.4	9	12.3	5	6.9	2	2.7	4.055	1.026	81.1
Y_2	22	30.1	39	53.4	5	6.9	4	5.5	3	4.1	4	0.986	80.0
Y_3	19	26	36	49.3	10	13.7	6	8.2	2	2.7	3.877	0.985	77.5
Y_4	18	24.7	28	38.4	16	21.9	9	12.3	2	2.7	3.699	1.063	74.0
Y_5	20	27.4	34	46.6	8	11	7	9.5	4	5.5	3.808	1.114	76.2
Y_6	23	31.5	25	34.2	12	16.4	10	13.7	3	4.1	3.753	1.164	75.1
Y_7	25	34.2	29	39.7	12	16.4	4	5.5	3	4.1	3.945	1.053	78.9
Y_8	19	26	34	46.6	10	13.7	6	8.2	4	5.5	3.795	1.092	75.9
Y_9	19	26	33	45.2	11	15.1	6	8.2	4	5.5	3.781	1.096	75.6
Y_10	27	37	29	39.7	10	13.7	4	5.5	3	4.1	4	1.054	80.0
الثقة الرقمية	%30.3		%43.2		%14.0		%8.4		%4.1		3.871	1.063	77.4
	%73.5						%12.5						

المصدر: إعداد الباحثين بالاعتماد على مخرجات برنامج SPSS V26.

يوضح الجدول (4) الخاص بوصف فقرات الثقة الرقمية ان المؤشر الكلي في جانب الاتفاق للأفراد المبحوثين بلغ (73.5%) بينما بلغت نسبة الافراد المحايدين (14%) وجاءت نسبة الإجابات للأفراد غير المتفقين (12.5%) ويدعم هذه الإجابات قيمة الوسط الحسابي البالغ (3.871).

ثانياً: اختبار التوزيع الطبيعي لمتغيرات الدراسة

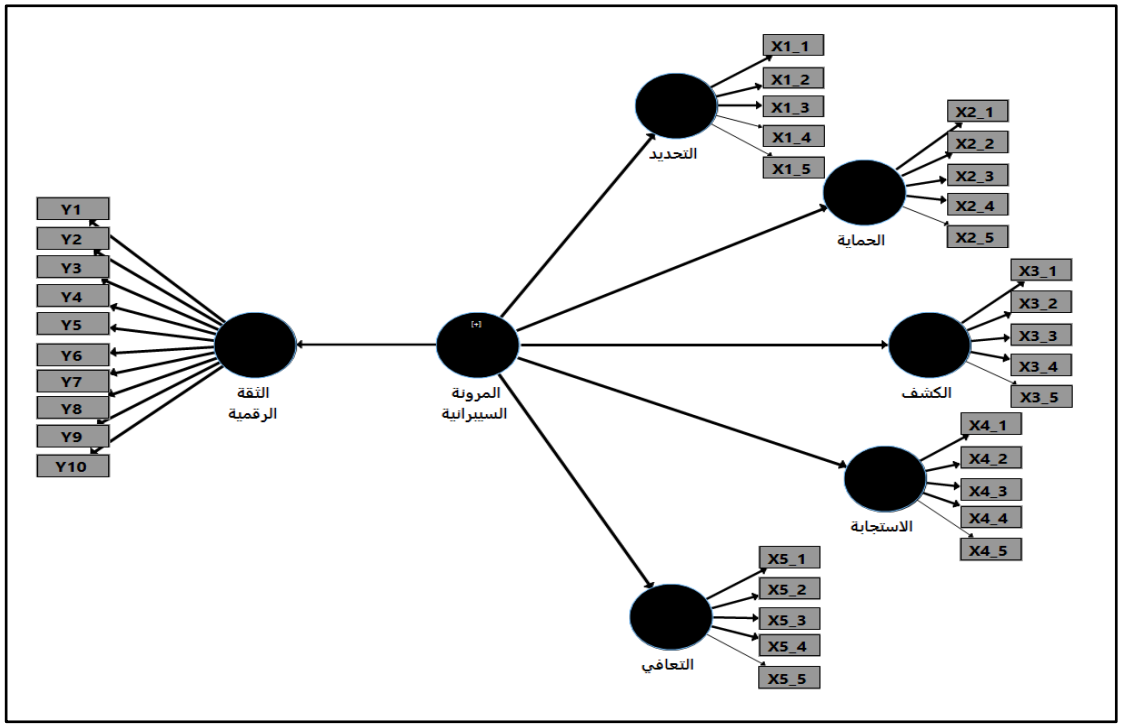
تم استخدام اختبار كولموكروف سميرنوف Kolmogorov-Smirnov، لاختبار التوزيع الطبيعي لمتغيرات الدراسة؛ وذلك لأن حجم العينة يزيد عن 50، ويكون هذا الاختبار مناسباً لاختبار التوزيع الطبيعي لهكذا أحجام عينات (Mishra et al., 2019: 70)، وكما يأتي:

جدول (5): نتائج اختبارات التوزيع الطبيعي

المتغير	البعد	Kolmogorov-Smirnov	
		إحصاءة الاختبار	Sig.
المرونة السيبرانية	التحديد	0.125	0.007
	الحماية	0.140	0.001
	الكشف	0.155	0.000
	الاستجابة	0.129	0.004
	التعافي	0.147	0.001
	المرونة السيبرانية	0.107	0.038
الثقة الرقمية		0.138	0.001

المصدر: إعداد الباحثين بالاعتماد على مخرجات برنامج SPSS V26.

يتضح من الجدول (5) أن أن هذه المتغيرات لا تتبع التوزيع الطبيعي وذلك لأن قيم Sig جميعها أقل من مستوى المعنوية 0.05 وهذه إحدى مبررات استعمالنا لنمذجة PLS-SEM وبالاعتماد على برنامج Smart PLS V3 تم رسم نموذج الدراسة وكما في الشكل (2).



شكل (2): نموذج الدراسة

المصدر: إعداد الباحثين بالاعتماد على برنامج Smart PLS V3.

ثالثاً: مراحل ومعايير تقييم نموذج الدراسة

يتم تقييم نموذج الدراسة وفقاً لمنهجية PLS-SEM من خلال مرحلتين. المرحلة الأولى تتعلق بتقييم واختبار العلاقات الترابطية بين متغيرات الدراسة الفقرات المتعلقة بها، وهذه المرحلة تعرف بالتقييم القياسي للنموذج. أما الثانية، فتركز على تقييم جودة واختبار العلاقات بين المتغيرات الكامنة في نموذج الدراسة التي ترتبط ببعضها بعضاً. وهذه المرحلة تسمى بمرحلة التقييم الهيكلي للنموذج. يتم تنفيذ عملية التقييم وفقًا للإرشادات والإجراءات المحددة في منهجية PLS-SEM، التي ذكرت في (Hair et al., 2022: 116-126) بشكل تفصيلي وقد تم تلخيصه في جدول واحد شامل من لدن (علي وآخرون، 2024: 496).

1- التقييم القياسي للنموذج:

تهدف هذه المرحلة إلى ضمان صدق واستقرار المتغيرات والمؤشرات من خلال النموذج.

أ. ثبات المؤشرات والأبعاد

يلخص الجدول (6) مقاييس الثبات لفقرات وأبعاد الدراسة

جدول (6): معايير تقييم النموذج

المتغير الكامن	المؤشرات	التحميلات الخارجية		الاتساق الداخلي		
		0.7 ≤	ملاحظة	AVE≥0.5	كرونباخ ألفا 0.7<	الثبات المركب
التحديد	X1_1	0.709	احتفاظ	0.651	0.864	0.903
	X1_2	0.883	احتفاظ			
	X1_3	0.839	احتفاظ			
	X1_4	0.737	احتفاظ			
	X1_5	0.853	احتفاظ			
الحماية	X2_1	0.761	احتفاظ	0.681	0.883	0.914
	X2_2	0.822	احتفاظ			
	X2_3	0.839	احتفاظ			
	X2_4	0.862	احتفاظ			
	X2_5	0.837	احتفاظ			
الكشف	X3_1	0.749	احتفاظ	0.543	0.783	0.852
	X3_2	0.798	احتفاظ			
	X3_3	0.819	احتفاظ			
	X3_4	0.779	احتفاظ			
	X3_5	0.774	احتفاظ			
الاستجابة	X4_1	0.714	احتفاظ	0.622	0.847	0.891

			احتفاظ	0.830	X4_2	
			احتفاظ	0.790	X4_3	
			احتفاظ	0.786	X4_4	
			احتفاظ	0.818	X4_5	
0.915	0.884	0.684	احتفاظ	0.785	X5_1	التعافي
			احتفاظ	0.862	X5_2	
			احتفاظ	0.753	X5_3	
			احتفاظ	0.887	X5_4	
			احتفاظ	0.840	X5_5	
0.964	0.960	0.522	**المرونة السيبرانية**			
0.933	0.920	0.581	احتفاظ	0.743	Y_1	الثقة الرقمية
			احتفاظ	0.790	Y_2	
			احتفاظ	0.775	Y_3	
			احتفاظ	0.764	Y_4	
			احتفاظ	0.836	Y_5	
			احتفاظ	0.750	Y_6	
			احتفاظ	0.702	Y_7	
			احتفاظ	0.790	Y_8	
			احتفاظ	0.717	Y_9	
			احتفاظ	0.743	Y_10	

المصدر: إعداد الباحثين بالاعتماد على برنامج Smart PLS V3.

نلاحظ من الجدول (6) أنه سيتم الاحتفاظ بجميع المؤشرات؛ والسبب في ذلك أن قيم التحميلات الخارجية لها أكبر من الحد المقبول 0.7، كما نلاحظ أن الأبعاد تتصف بالثبات بالاعتماد على قيم معاملات كرونباخ ألفا والثبات المركب ومعدل التباين المستخلص Average Variance Extracted (AVE).

ب. الصدق التمييزي لنموذج القياس

سيتم التحقق من أن المؤشرات التي تستخدم لقياس متغير كامن معين لا تقوم بقياس متغير كامن آخر، وذلك عن طريق استخدام الصدق التمييزي في نموذج القياس. ولتقدير الصدق التمييزي، يتم الاعتماد عادة على عدة معايير أهمها معيار HTMT (Heterotrait-Monotrait Ratio)، وكما يأتي:

جدول (7): نتائج معيار HTMT

	الاستجابة	التحديد	التعافي	الثقة الرقمية	الحماية	الكشف
التحديد	0.805					
التعافي	0.760	0.693				
الثقة الرقمية	0.795	0.762	0.800			
الحماية	0.765	0.803	0.802	0.809		
الكشف	0.729	0.800	0.764	0.686	0.813	
المرونة السيبرانية	0.834	0.837	0.804	0.811	0.842	0.838

المصدر: إعداد الباحثين بالاعتماد على برنامج Smart PLS V3.

يتضح من الجدول (7) قيم معيار جميعها أقل من المستوى المقبول 0.9 عند كل متغير مما يشير إلى صحة التمييز بين المتغيرات المدروسة فيما بينها وعدم تشابهها وهذا يعني أن كل متغير يمثل نفسه.

2- تقييم النموذج الهيكلي

تتم مرحلة تقييم النموذج الهيكلي من خلال تقييم العلاقات المفترضة في النموذج، بالاعتماد على عدة معايير أهمها (R^2 وF^2) كما سيتم تشخيص مشكلة التعدد الخطي بين المتغيرات المستقلة من خلال ما يسمى بمعيار معامل تضخم التباين (VIF) Variance Inflation Factor، وكما يأتي:

أ. معامل تضخم التباين (VIF)

جدول (8): معاملات تضخم التباين

المؤشر	X1_1	X1_2	X1_3	X1_4	X1_5
VIF	2.140	3.015	2.252	1.987	2.509
المؤشر	X2_1	X2_2	X2_3	X2_4	X2_5
VIF	1.970	2.541	3.155	3.679	2.452
المؤشر	X3_1	X3_2	X3_3	X3_4	X3_5
VIF	1.320	2.144	2.431	1.775	1.787
المؤشر	X4_1	X4_2	X4_3	X4_4	X4_5
VIF	1.469	2.052	1.812	1.836	1.880
المؤشر	X5_1	X5_2	X5_3	X5_4	X5_5
VIF	1.941	2.495	1.813	2.985	2.344
المؤشر	Y1	Y2	Y3	Y4	Y5
VIF	2.521	2.228	2.838	2.499	3.054
المؤشر	Y6	Y7	Y8	Y9	Y10
VIF	3.215	3.158	2.548	3.288	2.170

المصدر: إعداد الباحثين بالاعتماد على برنامج Smart PLS V3.

وتشير نتائج معيار VIF إلى انعدام وجود مشكلة التعدد الخطي فجميع قيم VIF هي أقل من 5.

ب. تقييم جودة النموذج

يتم تقييم جودة النموذج بالاعتماد على كل من (R^2 وF^2)، وكما يأتي:

جدول (9): قيم معايير جودة النموذج

المتغير	R^2	القدرة التفسيرية	F^2	حجم التأثير
التحديد	0.850	قوية	5.664	مرتفع
الحماية	0.906	قوية	9.618	مرتفع
الكشف	0.781	قوية	3.572	مرتفع
الاستجابة	0.787	قوية	3.705	مرتفع
التعافي	0.790	قوية	3.771	مرتفع
الثقة الرقمية	0.816	قوية	4.421	مرتفع

المصدر: إعداد الباحثين بالاعتماد على برنامج Smart PLS V3.

نلاحظ من الجدول (9) أن القدرة التفسيرية لجميع المسارات هي قوية، بمعنى لا يوجد معامل تحديد يقل عن 0.75 مما يدل على جودة النموذج بالاعتماد على هذا المعيار، ويؤيد ذلك معيار F^2، حيث إن جميع قيم هذا المعيار هي مرتفعة.

رابعاً: اختبار فرضيات الدراسة

1- اختبار الفرضية الرئيسة الأولى

حيث سيتم اختبار الفرضية الرئيسة الأولى التي تنص على ((**لا توجد علاقة ذات دلالة إحصائية بين المرونة السيبرانية والثقة الرقمية**))، والجدول (10) يوضح نتائج معامل الارتباط الذي يشير إلى رفض فرضية العدم والقبول بالبديلة لأن قيمة P-Value أقل من 0.05، مما يعني أنه توجد علاقة بين المرونة السيبرانية والثقة الرقمية.

جدول (10): علاقة الارتباط بين متغيري المرونة السيبرانية والثقة الرقمية

المتغيرات		والثقة الرقمية
المرونة السيبرانية	معامل الارتباط	0.903
	Sig	<0.001

المصدر: إعداد الباحثين بالاعتماد على برنامج Smart PLS V3.

2- اختبار الفرضية الفرعية للفرضية الرئيسة الأولى

سيتم اختبار الفرضية الفرعية للفرضية الرئيسة الأولى التي تنص على ((**لا توجد علاقة ذات دلالة إحصائية بين أبعاد المرونة السيبرانية والثقة الرقمية**)) حيث يتضمن الجدول (11) معامل ارتباط بيرسون والمعنوية المرافقة له للعلاقة بين كل بعد من أبعاد المرونة السيبرانية والثقة الرقمية، حيث تشير النتائج إلى رفض الفرضية والقبول بالبديلة التي تشير إلى وجود علاقة معنوية بين كل بعد من أبعاد المرونة السيبرانية والثقة الرقمية.

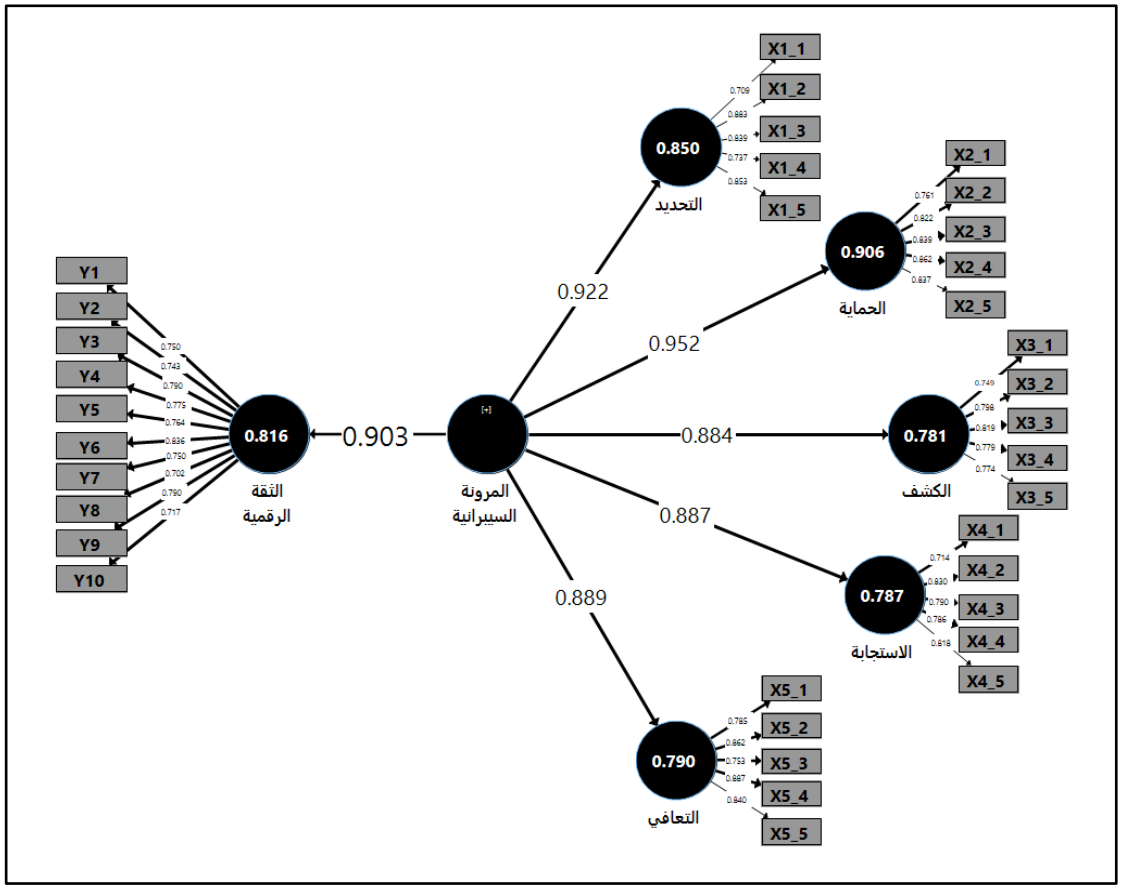
جدول (11): علاقة الارتباط بين أبعاد المرونة السيبرانية والثقة الرقمية

البعد	معامل الارتباط	P-Value
التحديد	0.808	<0.001
الحماية	0.861	<0.001
الكشف	0.717	<0.001
الاستجابة	0.829	<0.001
التعافي	0.862	<0.001

المصدر: إعداد الباحثين بالاعتماد على برنامج Smart PLS V3.

3- اختبار الفرضية الرئيسة الثانية

لغرض التأكد من الفرضيات الرئيسة الثانية التي تنص على ((**لا يوجد تأثير ذي دلالة إحصائية للمرونة السيبرانية في الثقة الرقمية**)) والتحقق من صحتها تم وضع نموذج (PLS-SEM) لإثبات أو نفي هذه الفرضيات باستعمال برنامج Smart-PLS 3، والشكل (3) يعرض رسم النموذج الخاص بهذه الفرضية، كما يظهر الجدول (10) نتائج تحليل الانحدار الخاصة بالنموذج التي تشير إلى رفض الفرضية الرئيسة الثانية.



شكل (3): تأثير المرونة السيبرانية في الثقة الرقمية

المصدر: إعداد الباحثين بالاعتماد على برنامج Smart PLS V3.

جدول (12): نتائج تأثير المرونة السيبرانية في الثقة الرقمية

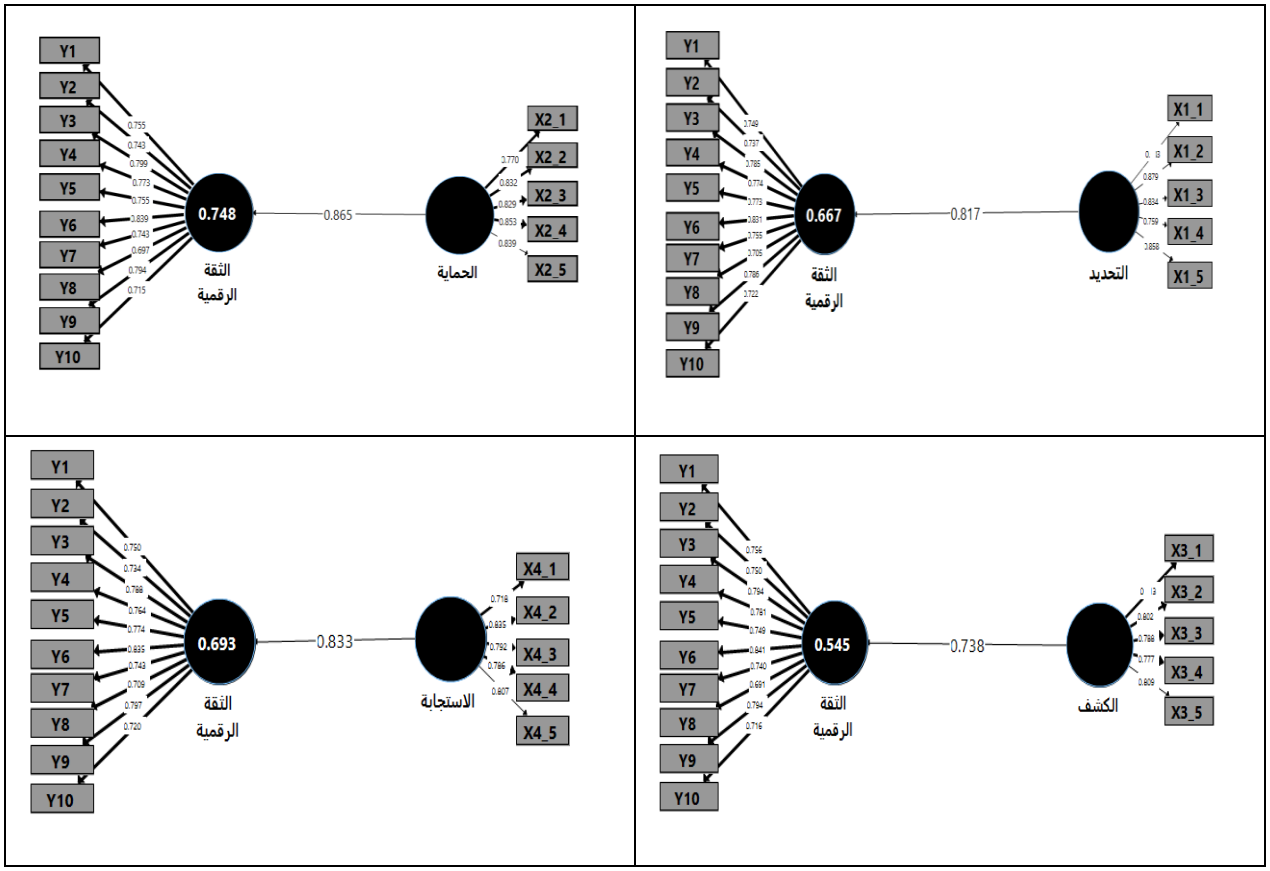
المتغير المعتمد: الثقة الرقمية				
المتغير المستقل	**معامل التأثير**	**قيمة t**	**P-Value**	**معامل التحديد**
المرونة السيبرانية	0.903	35.352	<0.001	%81.6

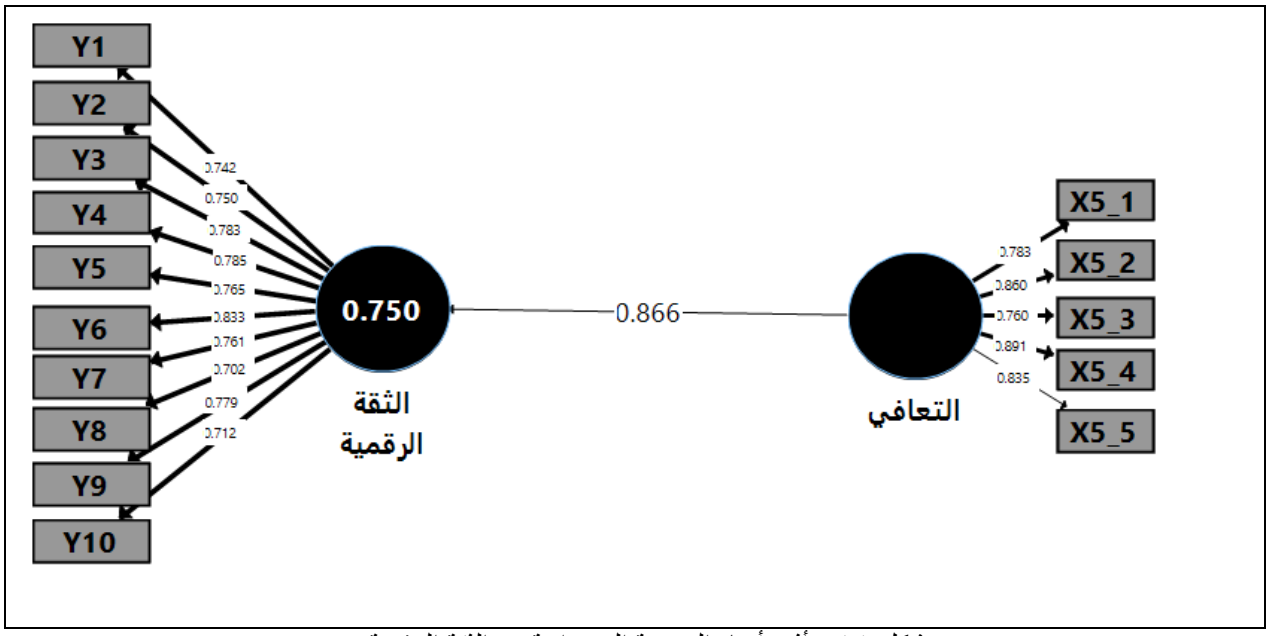
المصدر: إعداد الباحثين بالاعتماد على برنامج Smart PLS V3.

ونلاحظ من الجدول (12) أننا نرفض الفرضية الرئيسة الثانية؛ وذلك لأن قيمة P-Value أقل من مستوى المعنوية (0.05)، مما يعني بأن هناك تأثيراً معنوياً للمرونة السيبرانية في الثقة الرقمية، وتشير قيمة معامل التحديد أن هذا التأثير يفسر أكثر من 81%.

4- اختبار الفرضية الفرعية للفرضية الرئيسة الثانية

حيث سيتم اختبار الفرضية الفرعية للفرضية الرئيسة الثانية الخاصة بأبعاد متغير المرونة السيبرانية مع الثقة الرقمية، والشكل (4) يعرض رسم النماذج الخاصة بهذه الفرضية، كما يظهر الجدول (13) نتائج تحليل الانحدار الخاصة بهذه النماذج.





شكل (4): تأثير أبعاد المرونة السيبرانية في الثقة الرقمية

المصدر: إعداد الباحثين بالاعتماد على برنامج Smart PLS V3.

جدول (13): نتائج تأثير أبعاد المرونة السيبرانية في الثقة الرقمية

المتغير المعتمد: الثقة الرقمية				
المتغير المستقل	**معامل التأثير**	**قيم t**	**P-Value**	**معامل التحديد**
التحديد	0.817	19.81	<0.001	%66.7
الحماية	0.865	32.752	<0.001	%74.8
الكشف	0.738	15.873	<0.001	%54.5
الاستجابة	0.833	29.757	<0.001	%69.3
التعافي	0.866	32.415	<0.001	%75.0

المصدر: إعداد الباحثين بالاعتماد على برنامج Smart PLS V3.

ونلاحظ من الجدول (13) أننا نرفض الفرضية الفرعية للفرضية الرئيسة الثانية؛ وذلك لأن قيم P-Value أقل من مستوى المعنوية (0.05)، مما يعني بأن هناك تأثيراً معنوياً إحصائياً لكل بعد من أبعاد متغير المرونة السيبرانية في الثقة الرقمية، وإن

أعلى بعد من حيث نسبة التفسير هو بعد (التعافي) الذي يفسر 75%، وأن أقل بعد من حيث التأثير هو بعد (الكشف) بنسبة تفسير تساوي (54.5%).

الفصل الخامس: الاستنتاجات والتوصيات

أولا: الاستنتاجات

1- تُعد المرونة السيبرانية عاملاً حاسمًا في تعزيز مستوى الثقة الرقمية داخل البنك المركزي العراقي / فرع الموصل، إذ أن العلاقة بين المتغيرين علاقة طردية قوية ومعنوية بما يعكس اعتماد مستويات الثقة الرقمية على قدرة المنظمات في إدارة أبعاد المرونة السيبرانية بصورة فعّالة.

2- ان ارتفاع تأثير بُعد "التعافي" أهمية يفسر قدرة المنظمة على استرجاع عمل الأنظمة بسرعة بعد الحوادث السيبرانية، الأمر الذي يعزز شعور الأفراد بالثقة في البيئة الرقمية ويقلل من التردد في التعامل الإلكتروني.

3- يشير التأثير القوي لبُعد "الحماية" إلى أن وجود تدابير وقائية فعالة، مثل الجدران النارية وأنظمة التشفير والسياسات الأمنية، يسهم في ترسيخ ثقة المستخدمين بالمنصات الرقمية الخاصة بالبنك.

4- تبرز نتائج بُعد "الاستجابة" عاملاً مهماً، حيث يُظهر أن قدرة المنظمة على التعامل السريع والمنهجي مع الحوادث السيبرانية تُعد عنصرًا جوهريًا في بناء ثقة داخلية وخارجية بقدرات البنك التقنية والتنظيمية.

5- بينت نتائج بُعد "التحديد" أن توفر إطار واضح لتحديد الأصول الرقمية والتهديدات المحتملة يسهم بشكل واضح في دعم مستويات الثقة، من خلال تعزيز وضوح الأدوار والمسؤوليات وتوقع المخاطر.

6- بالرغم من أن بُعد "الكشف" كان الأقل تأثيرًا نسبيًا بين الأبعاد، إلا أنه لا يزال يظهر علاقة معنوية ومهمة بالثقة الرقمية، مما يشير إلى الحاجة لتعزيز أنظمة المراقبة المبكرة وتحسين أدوات التنبيه والرصد للكشف عن التهديدات قبل تفاقمها.

ثانيا: التوصيات

1- تعزيز قدرات البنك في وضع خطط الطوارئ وتدريب الكوادر على آليات استعادة البيانات وتشغيل الأنظمة الحرجة بسرعة بعد الهجوم السيبراني، بما يضمن تقليل زمن الانقطاع وبالتالي تعزيز الثقة الرقمية.

2- توسيع نطاق التدابير الوقائية عبر اعتماد بروتوكولات أمنية محدثة بشكل دوري، وتطبيق تقنيات تشفير متقدمة لضمان سلامة المعلومات والاتصالات.

3- زيادة فعالية الاستجابة للأحداث السيبرانية من خلال تأسيس فرق طوارئ متخصصة مزودة بإمكانات فنية وقرارات سريعة للتعامل مع الحوادث بشكل مباشر دون تأخير.

4- تبني تقنيات الذكاء الاصطناعي والتعلم الآلي لرصد الأنماط غير الطبيعية وتنبيه المسؤولين مبكرًا قبل تصاعد الهجمات السيبرانية.

5- إدراج المرونة السيبرانية ضمن الاستراتيجية العامة للبنك كعنصر من عناصر الحوكمة الرقمية، بما يضمن تكاملها مع باقي السياسات الإدارية والتقنية.

6- نشر ثقافة الأمن السيبراني بين الموظفين والمستفيدين من خدمات البنك عبر ورش عمل ودورات تثقيفية، تهدف إلى رفع وعي الأفراد بأهمية حماية البيانات والثقة الرقمية، وتعزيز التفاعل الإيجابي مع النظم الإلكترونية.

قائمة المصادر

أولا: المصادر العربية

1. علي، محمد حيدر، البجاري، أحمد يوسف، السنجاري، عدنان مصطفى، (2024)، "اليقظة التسويقية وإسهامها في تحقيق السيادة الاستراتيجية: دراسة مسحية لآراء عينة من القيادات الإدارية في شركة آسيا سيل للاتصالات المتنقلة في العراق"، مجلة الكوت للعلوم الاقتصادية والإدارية، المجلد 16، العدد 50، ص 484-507.

ثانيا: المصادر الاجنبية

1. Ahn, G., Jang, J., Choi, S., & Shin, D. (2024). Research on Improving Cyber Resilience by Integrating the Zero Trust security model with the MITRE ATT&CK matrix. *IEEE Access*.
2. Alhidaifi, S. M., Asghar, M. R., & Ansari, I. S. (2024). A survey on cyber resilience: Key strategies, research challenges, and future directions. *ACM computing surveys*, *56*(8), 1-48.
3. Aljumaiah, O., Jiang, W., Addula, S. R., & Almaiah, M. A. (2025). Analyzing cybersecurity risks and threats in IT infrastructure based on NIST framework. *Journal of Cyber Security and Risk Auditing*, *2025*(2), 12-26.
4. Anderson, R., Barton, C., Bölme, R., Clayton, R., Ganán, C., Grasso, T .& Vasek, M. (2019). Measuring the changing cost of cybercrime.
5. Asante, M., Epiphaniou, G., Maple, C., Al-Khateeb, H., Bottarelli, M., & Ghafoor, K. Z. (2021). Distributed ledger technologies in supply chain security management: A comprehensive survey. *IEEE Transactions on Engineering Management*, *70*(2), 713-739.
6. Bhatnagar, S. (2025). Digital Trust Certification: Building Resilient, Ethical, and Citizen-Centric Digital System.

7. Carayannis, E. G., Grigoroudis, E., Rehman, S. S., & Samarakoon, N. (2019). Ambidextrous cybersecurity: The seven pillars (7Ps) of cyber resilience. *IEEE transactions on engineering management*, *68*(1), 223-234.

8. Charter of Trust. (2025, February 14). Hybrid threats: An expert's playbook on cybersecurity. Agora Strategy Group AG & Kekst CNC.

9. Chen, K., Launer, M., Scarlat, C., & Guerrero-Cusumano, J. L. (2023). Trust and Digital Business: Theory and Practice.

10. Chui, K. T. (2023). Building digital trust: Challenges and strategies in cybersecurity. *Cyber Security Insights Magazine, Insights2Techinfo*, *5*, 15-18.

11. Costigan, S. S., & Ni Thuama, R. (2023). The State of Cyber Resilience 2023. *Red Sift| November*.

12. Guo, Y. (2022). Digital trust and the reconstruction of trust in the digital society: An integrated model based on trust theory and expectation confirmation theory. *Digital Government: Research and Practice*, *3*(4), 1-19.

13. Hair Jr, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). A primer on partial least squares structural equation modeling (PLS-SEM). 3rd Edition, Sage publications.

14. Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, *11*, 100204.

15. Jhonson, D., Smith, J., & Shehzadi, T. (2023). Digital Trust and Financial Transactions: Building Confidence in Internet Banking Systems.

16. Keleba, H., Tabona, O., & Maupong, T. (2022, November). Developing a Cyber-resilience state in Botswana's Energy Industry. In *2022 International Conference on Smart Applications, Communications and Networking (SmartNets)* (pp. 1-6). IEEE.

17. Kott, A., Blakely, B., Henshel, D., Wehner, G., Rowell, J., Evans, N., ... & Møller, A. (2018). Approaches to enhancing cyber resilience: Report of the north atlantic treaty organization (NATO) workshop IST-153. *arXiv preprint arXiv:1804.07651*.

18. Malik, P. K. (2024). The Role of Digital Trust in Enhancing Cyber Security Resilience. In *Transforming Industry using Digital Twin Technology* (pp. 59-67). Cham: Springer Nature Switzerland.

19. McClimans, F., Fersht, P., Snowdon, J., Phelps, B., & LaSalle, R. (2016). The State of Cybersecurity and Digital Trust, 2016. *Retrieved on January*, *12*, 2018.
20. Mishra, P., Pandey, C. M., Singh, U., Gupta, A., Sahu, C., & Keshri, A. (2019). Descriptive statistics and normality tests for statistical data. Annals of cardiac anaesthesia, 22(1), 67-72.
21. Nafees, M., & Kumar, M. M. CYBERSECURITY AND PRIVACY TRUST IN DIGITAL DATA: NAVIGATING THE DIGITAL TRUST LANDSCAPE.
22. Preecha, J. (2025, May). Cybersecurity and Public Trust in Digital Governance: Focusing on Citizen Trust. In *Proceeding of International Conference on Social Science and Humanity* (Vol. 2, No. 2, pp. 26-37).
23. PwC. (2024). Global digital trust insights: Bridging the gaps to cyber resilience – The C-suite playbook. PricewaterhouseCoopers.
24. Renckens, P., Ferentinos, L., & Wielart, A. (2024). Never Waste a Good Crisis: The Six Success Factors of Cyber Resilience.
25. Roshanaei, M. (2021). Resilience at the core: critical infrastructure protection challenges, priorities and cybersecurity assessment strategies. *Journal of Computer and Communications*, *9*(8), 80-102.
26. Safitra, M. F., Lubis, M., & Kurniawan, M. T. (2023, March). Cyber resilience: research opportunities. In *Proceedings of the 2023 6th international conference on electronics, communications and control engineering* (pp. 99-104).
27. Sailio, M., Latvala, O. M., & Szanto, A. (2020). Cyber threat actors for the factory of the future. *Applied Sciences*, *10*(12), 4334.
28. Saveljeva, J., & Volkova, T. (2025). A Survey on Digital Trust: Towards a Validated Definition.
29. Siddiqui, F., Hagan, M., & Sezer, S. (2019, September). Establishing cyber resilience in embedded systems for securing next-generation critical infrastructure. In *2019 32nd IEEE International System-on-Chip Conference (SOCC)* (pp. 218-223). IEEE.
30. Smith, S. (2023, March). Towards a scientific definition of cyber resilience. In *International Conference on Cyber Warfare and Security* (Vol. 18, No. 1, pp. 379-386). Academic Conferences International Limited.

31. Szumski, O. (2020). Technological trust from the perspective of digital payment. *Procedia Computer Science*, *176*, 3545-3554.
32. Teodoro, N., Gonçalves, L., & Serrão, C. (2015, August). NIST cybersecurity framework compliance: A generic model for dynamic assessment and predictive requirements. In *2015 IEEE Trustcom/BigDataSE/ISPA* (Vol. 1, pp. 418-425). IEEE.
33. Thompson, M. A., Ryan, M. J., & McLucas, A. C. (2015, April). A proposed resilience framework. In *Systems Engineering and Test and Evaluation (SETE) Conference, Canberra, AS* (pp. 27-29).
34. Verma, P., Newe, T., O'Mahony, G. D., Brennan, D., & O'Shea, D. (2025). Towards a Unified Understanding of Cyber Resilience: A Comprehensive Review of Concepts, Strategies, and Future Directions. *IEEE Access*.
35. Wang, H., Kang, X., Li, T., Lei, Z., Chu, C.-K., & Wang, H. (2023). An overview of trust standards for communication networks and future digital world. IEEE Access, 11, 42991–42998.
36. World Economic Forum, & University of Oxford. (2025). The cyber resilience compass: Journeys towards resilience (White Paper). World Economic Forum.
37. Yacoubian, L. J. (2025). Trust in digital banking: A thematic review of drivers, barriers and emerging evidence in developing countries. World Journal of Advanced Research and Reviews, 26(2), 4141–4147.