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

Cyber Resilience and its Impact on Improving the Quality of Digital Financial Services: An Applied Study at the Jordanian National Cyber Security Center

Shaima Mohammed Amin Al-Duwairi*[A], Zahraa Karim Jabbar [B], Taiba Haitham Saleh [C]

[A] Yarmouk University, Jordan
[B] Al Rasheed Bank/Talbia Branch
[C] College of Law/Future University

Keywords:
Cyber resilience, financial services quality, Jordanian National Cybersecurity Center.

Article history:
Received 15 Dec. 2024
Accepted 10 Jan. 2025
Available online 25 Jun. 2025

*Corresponding author:
Shaima Mohammed Amin Al-Duwairi
Yarmouk University, Jordan

Abstract: study examines the concept of cyber resilience and its role in enhancing the quality of digital financial services, with a specific focus on an applied case study at the Jordanian National Cyber Security Center (JNCSC). As the reliance on digital platforms for financial services continues to increase, ensuring the robustness and reliability of cybersecurity measures becomes critical to safeguarding financial transactions and data. The study explores the various strategies implemented by the JNCSC to fortify cyber resilience and mitigate the risks associated with cyber threats in the financial sector. Through an analysis of both qualitative and quantitative data, the study assesses the effectiveness of these strategies in improving the operational efficiency, security, and trustworthiness of digital financial services. The findings indicate that robust cyber resilience frameworks significantly enhance service continuity, reduce downtime, and foster consumer confidence. The study concludes with recommendations for further strengthening cyber resilience in the context of digital financial services, aiming to improve their quality and sustainability in the long term.

المرونة السيبرانية وأثرها في تحسين جودة الخدمات المالية الرقمية دراسة تطبيقية في المركز الوطني للأمن السيبراني الأردني

شيماء محمد امين الدويري
جامعة اليرموك
الأردن

زهراء كريم جبار
مصرف الرشيد
فرع الطالبية

طيبة هيثم صالح
جامعة المستقبل
كلية القانون

المستخلص

تتناول هذه الدراسة مفهوم المرونة السيبرانية ودورها في تعزيز جودة الخدمات المالية الرقمية، مع التركيز بشكل خاص على دراسة حالة تطبيقية في المركز الوطني للأمن السيبراني الأردني. ومع استمرار الاعتماد على المنصات الرقمية في الخدمات المالية، فأن ضمان قوة وموثوقية تدابير الأمن السيبراني يصبح أمرًا بالغ الأهمية لحماية المعاملات والبيانات المالية. وتستكشف الدراسة الاستراتيجيات المختلفة التي ينفذها المركز الوطني للأمن السيبراني الأردني لتعزيز المرونة السيبرانية والتخفيف من المخاطر المرتبطة بالتهديدات السيبرانية في القطاع المالي. ومن خلال تحليل البيانات النوعية والكمية، تقيم الدراسة فعالية هذه الاستراتيجيات في تحسين الكفاءة التشغيلية والأمن والثقة في الخدمات المالية الرقمية. وتشير النتائج إلى أن أطر المرونة السيبرانية القوية تعمل بشكل كبير على تعزيز استمرارية الخدمة وتقليل وقت التوقف وتعزيز ثقة المستهلك. وتختتم الدراسة بتوصيات لتعزيز المرونة السيبرانية بشكل أكبر في سياق الخدمات المالية الرقمية، بهدف تحسين جودتها واستدامتها على المدى الطويل.

الكلمات المفتاحية: المرونة السيبرانية، جودة الخدمات المالية، المركز الوطني للأمن السيبراني الأردني.

المقدمة

في عالم رقمي يترابط بشكل متزايد، أحدث التطور السريع للتكنولوجيا المالية ثورة في طريقة تفاعل الأفراد والمنظمات مع الخدمات المالية. ومع ذلك، فأن فوائد التحول الرقمي مصحوبة بتحديات كبيرة، وخاصة فيما يتعلق بتهديدات الأمن السيبراني. تتطلب هذه التحديات تبني استراتيجيات قوية للمرونة السيبرانية لحماية البيانات الحساسة، وضمان استمرارية الخدمة، وتعزيز الثقة بين مستخدمي الخدمات المالية الرقمية.

تتجاوز المرونة السيبرانية، وهي نهج شامل لإدارة وتخفيف المخاطر السيبرانية، تدابير الأمن السيبراني التقليدية من خلال التأكيد على القدرة على توقع الأحداث السيبرانية السلبية ومقاومتها والتعافي منها والتكيف معها. وفي سياق الخدمات المالية الرقمية، تصبح هذه المرونة عاملاً حاسماً في حماية المعاملات وحماية معلومات المستخدم وضمان استقرار المنصات المالية.

تركز هذه الدراسة على دور المرونة السيبرانية في تعزيز جودة الخدمات المالية الرقمية، مع تطبيق محدد على المركز الوطني للأمن السيبراني الأردني. بصفته مؤسسة محورية في إطار الأمن السيبراني في الأردن، يلعب المركز الوطني للأمن السيبراني دورًا رئيسًا في إنشاء وصيانة آليات المرونة السيبرانية التي تؤثر بشكل مباشر على النظام البيئي المالي الرقمي في البلاد.

من خلال نهج تطبيقي، تهدف هذه الدراسة إلى استكشاف الاستراتيجيات التي يستخدمها المركز الوطني للأمن السيبراني لتعزيز المرونة السيبرانية، وتحليل آثارها على جودة وموثوقية

الخدمات المالية الرقمية، وتقديم توصيات قابلة للتنفيذ لأصحاب المصلحة. سيساهم هذا التحقيق في فهم أعمق لكيفية تعزيز ممارسات المرونة السيبرانية الفعالة للثقة والأمان والكفاءة في مجال التمويل الرقمي.

المحور الأول: المنهجية العلمية للدراسة

أولاً. مشكلة الدراسة: في ظل النظام المالي الرقمي سريع التطور، أصبح ضمان أمن وموثوقية الخدمات المالية مصدر قلق ملح. تلعب المرونة السيبرانية، التي تشمل القدرة على توقع التهديدات السيبرانية ومواجهتها والتعافي منها والتكيف معها، دورًا حاسمًا في الحفاظ على جودة الخدمات المالية الرقمية وتعزيزها. وعلى الرغم من أهميتها، إلا أن هناك نقصًا في البحوث التطبيقية الشاملة التي تستكشف التأثير المباشر لاستراتيجيات المرونة السيبرانية على جودة الخدمات المالية الرقمية في الأطر المؤسسية. وعلى وجه التحديد، لا يزال دور المركز الوطني للأمن السيبراني الأردني في تعزيز المرونة السيبرانية وتأثيره على تحسين جودة الخدمة داخل القطاع المالي الرقمي غير مستكشف. يحاول هذا البحث سد هذه الفجوة من خلال التحقيق في الآثار العملية للمرونة السيبرانية على تحسين جودة الخدمة. لذا تتلخص مشكلة الدراسة في اثارة الأسئلة الآتية:

1. ما هي المرونة السيبرانية، ولماذا هي ضرورية للخدمات المالية الرقمية؟
2. كيف تساهم الهيئة الوطنية للأمن السيبراني في تعزيز المرونة السيبرانية في القطاع المالي الرقمي في الأردن؟
3. ما هي الدروس التي يمكن تعلمها من تجربة الهيئة الوطنية للأمن السيبراني لإعلام تطوير أطر المرونة السيبرانية في البلدان الأخرى؟

ثانياً. أهداف الدراسة: تهدف الدراسة إلى استكشاف مفهوم المرونة السيبرانية وأهميتها في تعزيز جودة الخدمات المالية الرقمية. من خلال دراسة الممارسات والاستراتيجيات التي يطبقها المركز الوطني للأمن السيبراني في الأردن، سنتعمق في الطرق المحددة التي يمكن من خلالها تطبيق المرونة السيبرانية لتحسين أمن وموثوقية الأنظمة المالية الرقمية.

ثالثاً. أهمية الدراسة: تتمثل أهمية الدراسة بما يأتي:

1. مع الاعتماد المتزايد على الخدمات المالية الرقمية، زاد خطر التهديدات السيبرانية بشكل كبير. تستكشف هذه الدراسة كيف يمكن للمرونة السيبرانية أن تعمل كعامل محوري في التخفيف من هذه المخاطر وهي تتماشى مع الحاجة العالمية لتعزيز تدابير الأمن السيبراني، وخاصة في القطاعات الحيوية مثل التمويل.
2. تسلط التركيز على تحسين جودة الخدمات المالية الرقمية الضوء على الفوائد المباشرة لممارسات الأمن السيبراني القوية، مع التركيز على تجربة المستخدم الأفضل والثقة والكفاءة التشغيلية.
3. من خلال دراسة المركز الوطني للأمن السيبراني الأردني، تقدم الدراسة رؤى حول كيفية تنفيذ منظمة على المستوى الوطني لاستراتيجيات المرونة السيبرانية. ويمكن أن تكون بمثابة نموذج للدول والمنظمات الأخرى التي تسعى إلى تعزيز أطر الأمن الرقمي الخاصة بها.
4. تضمن الطبيعة التطبيقية للدراسة أن تكون النتائج قابلة للتنفيذ وذات صلة بممارسي الصناعة والمؤسسات المالية وصناع السياسات. كما تساهم الدراسة في الأدبيات الموجودة من خلال ربط المرونة السيبرانية بشكل مباشر بجودة الخدمة في القطاع المالي، مما يوفر منظورًا فريدًا حول الترابط بين الأمن وتحسين الخدمة.

رابعاً. فرضيات الدراسة: فرضية الدراسة عبارة عن حل محتمل لمشكلة الدراسة وتنص فرضية الدراسة الرئيسة على: تؤثر المرونة السيبرانية بشكل كبير على جودة الخدمات المالية الرقمية في المركز الوطني للأمن السيبراني الأردني".

المحور الثاني: الإطار النظري للدراسة

المبحث الأول: الإطار النظري للمتغير المستقل المرونة السيبرانية

أولاً. مفهوم المرونة السيبرانية: مؤخراً تحولت المخاطر السيبرانية من مجرد إزعاجات إلى أحداث كارثية محتملة تهدد بقاء المنظمات المعتمدة على التكنولوجيا. وقد حدد المجلس العام لمجلس المخاطر النظامية الأوروبي، الذي يشرف على النظام المالي للاتحاد الأوروبي، المخاطر السيبرانية بعدّها "مصدرًا للمخاطر النظامية على النظام المالي" (ESRB 2020)، بناءً على الخوف من أن يتصاعد حادث الأمن السيبراني، مما يخلق أزمة سيولة من شأنها أن تؤدي إلى تآكل ثقة الجهات الفاعلة المالية وزعزعة استقرار النظام بأكمله. قد تبدو مثل هذه السيناريوهات الكارثية متطرفة، لكن تقريرًا صادرًا عن صندوق النقد الدولي في عام 2018، باستخدام البيانات المقدمة من جمعية تبادل بيانات المخاطر التشغيلية، يقدر أن الخسائر الإجمالية الناتجة عن الهجمات الإلكترونية على 7947 بنكًا في جميع أنحاء العالم بلغت 97 مليار دولار سنويًا (9% من صافي الدخل)، مع تذبذب القيمة المعرضة للخطر (VaR) بين 147 و201 مليار دولار (14% إلى 19% من صافي الدخل). وتظهر النماذج الأكثر تشاؤما خسائر سنوية تصل إلى 51% في ظل أكثر الظروف سوءا (Bouveret, 2018: 20-21). ولكي نفهم كيف يمكن للمخاطر السيبرانية أن تولد مثل هذه الصدمات المدمرة للبنى التحتية الحيوية التي نعتمد عليها، فلنتأمل الحالة التي حظيت بتغطية إعلامية واسعة النطاق لشركة الشحن العملاقة الدنماركية APM-Maersk. إن ما يثير الاهتمام هنا ليس تحديد هوية المهاجمين أو ما يقوله هذا الهجوم عن الحالة الحالية للصراع السيبراني (Arquilla & Ronfeldt, 2007; Rid, 2012; Rid & Buchanan, 2015) بل مدى التدمير الذي أحدثته مثل هذه الحوادث حتى بالنسبة لأكبر المنظمات وأكثرها نضجا، وكيف يقوم الضحايا بترقية نموذج إدارة مخاطر الأمن السيبراني التقليدي لديهم لاحتضان نموذج المرونة السيبرانية.

تُعَد شركة APM-Maersk، التي تشغل أكثر من 800 سفينة وتدير 76 محطة موانئ حول العالم، مسؤولة عن 20% من حركة الحاويات العالمية، مما يجعلها مركزًا رئيسيًا في نظام التجارة العالمي. في 27 يونيو 2017، أصيبت أنظمة الكمبيوتر الخاصة بالشركة ببرنامج خبيث، أطلق عليه لاحقًا قطاع الأمن السيبراني اسم NotPetya. انتشر NotPetya بسرعة غير مسبوقة وكان قادرًا على تجاوز ميزات الأمان حتى في الأنظمة المحدثة مؤخرًا وتشفير محتوياتها، مما يجعله أحد أكثر التهديدات الرقمية عدوانية التي لوحظت على الإطلاق (Greenberg, 2019: 183). تم استخدام NotPetya، المنسوب إلى قراصنة برعاية الدولة الروسية، في البداية ضد البنى التحتية الحيوية في أوكرانيا قبل أن ينتشر إلى مجموعة أوسع بكثير من الضحايا من الشركات، بما في ذلك بعضها في روسيا (NCSC, 2018). ورغم أن إصابة شركة ميرسك بالعدوى استغرقت أقل من سبع دقائق، فقد استغرق قطع الاتصال بشبكة الشركة العالمية بالكامل ما يقرب من ساعتين في محاولة عبثية لدرء الهجوم (Greenberg, 2019: 152).

قدمت إدارة ميرسك رواية صريحة ومفيدة عن كيفية تعاملها مع عواقب الهجوم. ورسم آدم بانكس، كبير مسؤولي التكنولوجيا والمعلومات في الشركة، صورة قاتمة للأضرار: 49 ألف جهاز

كمبيوتر وجهاز طباعة فضلا عن 56% من 6200 خادم و83% من 1200 تطبيق مطلوبة لتشغيل الأعمال كانت غير قابلة للتشغيل على الفور. وكانت خطوط الهاتف الثابتة اللازمة لتنسيق الاستجابة غير متاحة لأنها اعتمدت على شبكة الكمبيوتر، وتعطلت الهواتف المحمولة لأن جميع جهات الاتصال التي تستخدم Microsoft Outlook للمزامنة قد تم مسحها (Ritchie 2019). ولم يكن من الممكن استعادة نسخ احتياطية من البيانات المشفرة إذ احتاجت جميع خوادم وحدة التحكم في المجال إلى إعادة بناء خريطة للشبكة التي تعرضت للاختراق (Greenberg, 2019: 194). وكان أحد القرارات الأولى التي اتخذتها شركة ميرسك هو التخلي عن بروتوكول إدارة الأزمات الحالي، والذي لم يتضمن قط خططًا لمثل هذا المستوى الشامل من التدمير، وإعادة بناء شبكتها من الصفر بدلاً من ذلك، بمساعدة شركة استشارية حصلت على شيك مفتوح. وحصلت الشركة على فرصة محظوظة عندما اكتشفت أن انقطاع التيار الكهربائي في نيجيريا قد نجا من خادم واحد يمكن استخدامه لإعادة بناء الشبكة بالكامل. بدءًا من ذلك الجهاز الواحد، أعادت ميرسك في غضون 10 أيام تثبيت 2000 جهاز كمبيوتر محمول وفي غضون شهر أصدرت ما يقرب من 50000 جهاز نظيف للموظفين. وفي الوقت نفسه، تمكن الموظفون، الذين عادوا إلى القلم والورق وتلقي الطلبات عبر حسابات Gmail وWhatsApp الشخصية، من الحفاظ على 80% من حركة الحاويات (Crozier, 2018). وعلى الرغم من التكاليف الباهظة التي تكبدتها الشركة نتيجة للصدمة (بين 200 و250 مليون دولار أميركي)، فقد نجت الشركة، بل وتعززت سمعتها بفضل استعدادها لمشاركة الدروس المستفادة على طول الطريق. وصرح الرئيس التنفيذي للشركة بأن طموحه الجديد هو استخدام الحادث "للوصول إلى نقطة تصبح فيها قدرة [ميرسك] على إدارة الأمن السيبراني ميزة تنافسية" (Crozier, 2018). إن تجربة ميرسك تجسد المرونة السيبرانية في العمل: فعلى الرغم من مستوى الاستعداد الذي كان يُعتقد أنه كافٍ، أدى خطر غير متوقع إلى موقف لم يسبق مواجهته - أو حتى تخيله - ووجدت الشركة أن تدابير الأمن السيبراني الحالية قد غمرتها تمامًا. لعب الحظ دورًا في مواجهة هذا التحدي ولكنه لم يكن كافيًا إذا لم يحشد الموظفون من جميع أجزاء المنظمة ويبتكرون حلولاً مرتجلة للحفاظ على استمرار العمليات. كانت الموارد الخارجية ضرورية أيضًا، حيث ربما لم تتمكن ميرسك من إعادة بناء شبكتها في مثل هذا الوقت القصير بدون خبرة شركة الاستشارات التي استأجرتها. كانت الثقة وحسن النية التي تراكمت لدى ميرسك بين نظيراتها من الشركات مهمة أيضًا، إذ تمكنت من استخدام شبكات تكنولوجيا المعلومات الخاصة بها للتثبيتات الجديدة عندما نفد العرض المحلي من أقراص USB (Ritchie, 2019). أخيرًا، أدت هذه الصدمة الشديدة إلى عملية تكيف ناجحة لدرجة أن المنظمة تمكنت من الترويج لخبرتها الجديدة في مجال الأمن السيبراني في المنتدى الاقتصادي العالمي بعد عام (Olenick, 2018).

وعلى الرغم من أمثلة مثل هذه، والتاريخ الطويل لاستخدامها في مجالات علم المواد، والبيئة، وعلم النفس، واستخدامها المكثف مؤخرًا كاستراتيجية لمعالجة مخاطر عصر الأنثروبوسين (Boin and van Eeten, 2013)، فأن مفهوم المرونة لا يزال هامشيًا في الأدبيات المتعلقة بالمخاطر السيبرانية. وعندما يظهر، فأنه ينشأ في المقام الأول في مجال علوم الكمبيوتر، إذ تتعلق أسئلة البحث الرئيسية بتحديد السمات الهندسية التي يمكن أن تجعل الأنظمة السيبرانية أكثر قوة والمقاييس التي يمكن استخدامها لتقييم قدرتها على التحمل (Bodeau and Graubart, 2011; Linkov et al., 2013). وفي حين أن هذه الأمور مهمة، إلا أن هناك حاجة إلى نهج أكثر شمولاً

للمساعدة في فهم أنواع الاستعدادات والاستجابات والتعافي وأنشطة التكيف اللازمة لتعزيز المرونة السيبرانية للمنظمة (The National Academies, 2012).

ويمكن تعريف المرونة السيبرانية بأنها "القدرة على تحقيق النتيجة المقصودة على الرغم من الأحداث السيبرانية السلبية بشكل مستمر" (Björk et al., 2015: 312) ويميز هذا التعريف المرونة السيبرانية عن الأمن السيبراني، الذي يتمثل هدفه الرئيس في التنبؤ بالأحداث الضارة ومنعها. كما تشير المرونة السيبرانية إلى قدرة المؤسسة على الاستعداد للحوادث السيبرانية فضلا عن الاستجابة لها والتعافي منها مع الحفاظ على الوظائف الأساسية. وفي سياق الخدمات المالية، وخاصة داخل المؤسسات مثل المركز الوطني للأمن السيبراني الأردني، فأن تعزيز المرونة السيبرانية أمر بالغ الأهمية بسبب التكرار المتزايد وتعقيد الهجمات السيبرانية التي تستهدف هذا القطاع (Annarelli, & Palombi, 2021: 14).

ثانياً. أهمية المرونة السيبرانية: تتمثل أهمية المرونة السيبرانية في الخدمات المالية بما يأتي: (Petrenko, 2022: 159)

القطاع المالي معرض بشكل خاص للتهديدات السيبرانية، والتي يمكن أن تؤدي إلى اضطرابات تشغيلية كبيرة وخسائر مالية. إن التعقيد المتزايد لهذه الهجمات يتطلب استراتيجية قوية للمرونة السيبرانية لا تركز فقط على الوقاية ولكن أيضًا على التعافي والتكيف.. إذ يساعد هذا التركيز المزدوج على تحسين جودة الخدمات المالية الرقمية من خلال ضمان قدرة المؤسسات على الحفاظ على استمرارية الخدمة حتى في مواجهة الحوادث السيبرانية

المبحث الثاني: الإطار النظري للمتغير التابع جودة الخدمات المالية

أولاً. مفهوم جودة الخدمات المالية الرقمية: لقد غيرت الخدمات المالية الرقمية مشهد الشمول المالي وإمكانية الوصول إليه. إن جودة هذه الخدمات أمر بالغ الأهمية لضمان تلبية احتياجات المستخدمين بشكل فعال، وخاصة في المجتمعات المهمشة. يمكن أن تؤدي الخدمات المالية الرقمية عالية الجودة إلى تحسين الوصول إلى الحسابات المالية الرسمية، وخفض تكاليف المعاملات، وتعزيز رضا الزبائن (Sharma, & Díaz Andrade, 2023: 586). إذ حسنت الخدمات المالية الرقمية بشكل ملحوظ الوصول إلى الموارد المالية للسكان المحرومين. من خلال تسهيل الوصول إلى الحسابات الرسمية وخفض تكاليف التحويلات المالية، تساعد هذه الخدمات في التخفيف من حدة الفقر وتعزيز الاستقرار المالي للمجتمعات المهمشة. ويؤكد هذا التأثير على أهمية الحفاظ على خدمات عالية الجودة لضمان توزيع فوائد التمويل الرقمي على نطاق واسع (Ozili, 2018: 349).

وتشير جودة الخدمات المالية الرقمية إلى مدى فعالية وكفاءة ورضا المستخدمين عن هذه الخدمات. وتلبي الخدمات المالية الرقمية عالية الجودة توقعات الزبائن وتضمن الموثوقية وتخلق القيمة للأفراد والشركات(Luo, et al., 2022: 18).

كما تشير جودة الخدمات المالية الرقمية إلى مدى كفاءة وفعالية الخدمات المالية المقدمة من خلال الوسائل الرقمية في تلبية احتياجات العملاء وتوقعاتهم. مع التطور السريع في التكنولوجيا المالية (FinTech)، أصبحت جودة الخدمات الرقمية عاملاً حاسمًا لنجاح المؤسسات المالية في السوق(Bapat, 2022: 305) .

ثانياً. أبعاد جودة الخدمات المالية: تشمل الخدمات المالية الرقمية مجموعة واسعة من المنتجات والخدمات المالية المقدمة من خلال القنوات الرقمية. وتعتبر جودة هذه الخدمات أمرًا بالغ الأهمية

لضمان رضا الزبائن وتعزيز الشمول المالي. وفيما يأتي الأبعاد الرئيسة للجودة في الخدمات المالية الرقمية (Bankuoru Egala, et al, 2021: 148):

1. الوصول ودعم الزبائن: يشير هذا البعد إلى توافر الخدمات المالية الرقمية للمستخدمين، وخاصة الفئات المهمشة. ويشمل عوامل مثل النطاق الجغرافي للخدمات والبنية التحتية التكنولوجية الموجودة. إذ يعد ضمان الوصول الواسع أمرًا أساسيًا لتعزيز الشمول المالي وتمكين المستخدمين من الاستفادة من الخدمات المالية الرقمية. كما يندرج توافر وفعالية خدمات دعم الزبائن، بما في ذلك مكاتب المساعدة والمساعدة عبر الإنترنت، ضمن هذا البعد. إذ يعد دعم الزبائن الجيد أمرًا حيويًا لحل المشكلات بسرعة والحفاظ على رضا الزبائن.
2. الاستخدام: يقيس هذا البعد مدى تكرار وفعالية تفاعل المستخدمين مع الخدمات المالية الرقمية. ويعكس التبني الفعلي لهذه الخدمات واستخدامها من قبل المستهلكين. اذ تشير معدلات الاستخدام المرتفعة إلى أن الخدمات تلبي احتياجات المستخدمين وتندمج في سلوكياتهم المالية.
3. جودة البيانات: يركز هذا البعد على دقة واكتمال وموثوقية البيانات المستخدمة في الخدمات المالية الرقمية. وهو أمر بالغ الأهمية لاتخاذ القرارات الفعالة وإدارة المخاطر. إذ يمكن أن تؤدي جودة البيانات الرديئة إلى مخاطر تشغيلية كبيرة وتقويض ثقة الزبائن في الخدمات المالية. كما تشمل الجودة جوانب مختلفة من تقديم الخدمة، بما في ذلك الموثوقية والأمان وتجربة المستخدم. كما تتضمن استجابة الخدمة لاستفسارات وقضايا المستخدم. إذ تعمل الخدمات عالية الجودة على تعزيز ثقة المستخدم ورضاه، وهو أمر ضروري للمشاركة والولاء على المدى الطويل.

ثالثاً. تأثير المرونة السيبرانية على الخدمات المالية الرقمية: تتأثر جودة الخدمات المالية الرقمية بعدة عوامل، بما في ذلك سلامة البيانات وتجربة الزبائن ودورها في تعزيز الشمول المالي. ومع استمرار تطور المشهد المالي الرقمي، فأن التركيز على هذه الجوانب سيكون أمرًا بالغ الأهمية لتعظيم فوائد هذه الخدمات لجميع المستخدمين (Yadav, 2023: 57). إذ يمكن أن يؤدي تنفيذ تدابير المرونة السيبرانية الفعالة إلى العديد من النتائج الإيجابية للخدمات المالية الرقمية (Dupont, 2019: 34):

1. من خلال إظهار الالتزام بالأمن السيبراني، يمكن للمؤسسات المالية بناء الثقة مع الزبائن، وهو أمر ضروري لتبني الخدمات الرقمية.
2. تضمن استراتيجيات المرونة السيبرانية بقاء الخدمات الأساسية قيد التشغيل أثناء وبعد وقوع حادث سيبراني، ومن ثم تقليل الاضطرابات.
3. مع تشديد اللوائح المتعلقة بالأمن السيبراني على مستوى العالم، فأن وجود إطار قوي للمرونة السيبرانية يساعد المؤسسات على الامتثال للمتطلبات القانونية، مما يقلل من خطر العقوبات.
4. يتيح التركيز على المرونة للمؤسسات فهم وإدارة مخاطرها السيبرانية بشكل أفضل، مما يؤدي إلى اتخاذ قرارات أكثر استنارة وتخصيص الموارد.

المحور الثالث: الجانب الميداني للدراسة

أولاً. نبذة عن المركز المبحوث: المركز الوطني للأمن السيبراني هو جهة حكومية تسعى إلى إنشاء منظومة متكاملة وفعّالة للأمن السيبراني على المستوى الوطني، وتطويرها وتنظيمها لضمان حماية المملكة من تهديدات الفضاء السيبراني والتصدي لها بكفاءة وفعالية. يهدف المركز إلى تحقيق استدامة العمليات، وتعزيز الأمن الوطني، والحفاظ على سلامة الأفراد والممتلكات وحماية المعلومات ولغايات إيجاد فضاء سيبراني أردني آمن وموثوق، يسعى المركز إلى تدريب وتأهيل وتوعية وتثقيف

موظفي القطاع العام والخاص وفئات المجتمع كافة وإكسابهم المعرفة والمهارات اللازمة للحد من المخاطر والتهديدات وفقاً لأفضل الممارسات في مجال الأمن السيبراني وبما يضمن أعلى مستوى من الكفاءة، وجعل الأردن مركز إبداع وتميز إقليمي ودولي في هذا المجال.

استنادًا إلى قانون الأمن السيبراني رقم 16 لسنة 2019 والتي نصت المادة 6 منه على "ب- يتولى المركز في سبيل تحقيق أهدافه المهام والصلاحيات الآتية: تحديد شبكات البنى التحتية الحرجة ومتطلبات استدامتها "، وعلى ضوء تعريف البنى التحتية الحرجة الوارد في القانون " البنية التحتية الحرجة: مجموعة من الأنظمة والشبكات الإلكترونية، فضلا عن الأصول المادية وغير المادية أو الأصول السيبرانية، التي يعد تشغيلها المستمر أمراً ضرورياً لضمان أمن الدولة، واستقرار اقتصادها، وسلامة المجتمع. "، إذ أن القانون قد بين ماهية البنى التحتية الحرجة من خلال التعريف أعلاه وحدد أن البنى التحتية الحرجة هي في أصلها شبكات وأنظمة معلومات ترتبط ارتباط وثيق بأمن الدولة والاقتصاد وسلامة المجتمع فقد تم اعتماد المعايير الأساسية التالية والتي يكفي أن ينطبق أحدها على القطاع ليتم عدّه قطاع بنية تحتية حرجة:

1. أمن الدولة.
2. الاقتصاد.
3. سلامة المجتمع.

وعلى ضوء ما تقدم تم عدّ القطاعات الآتية قطاعات بنى تحتية حرجة: (الموقع الرسمي للمركز الوطني للأمن السيبراني)

1. قطاع الخدمات الحكومية
2. قطاع الصناعة والتجارة
3. القطاع المالي والمصرفي
4. قطاع الاتصالات وتكنولوجيا المعلومات
5. قطاع الطاقة
6. قطاع الصحة
7. قطاع الزراعة والمياه والبيئة
8. قطاع النقل
9. قطاع التعليم
10. قطاع الدفاع والأمن

ثانياً. الخدمات الرئيسة التي يقدمها المركز: يتولى المركز في سبيل تحقيق أهدافه ومن خلال نشاطاته وخدماته مهمة خلق منظومة وعي متكاملة عند الأفراد والمؤسسات وتطوير قدرات البحث العلمي بكل جوانب الأمن السيبراني من خلال الخدمات المتنوعة التي يقدمها وهي على النحو الآتي: (الموقع الرسمي للمركز الوطني للأمن السيبراني)

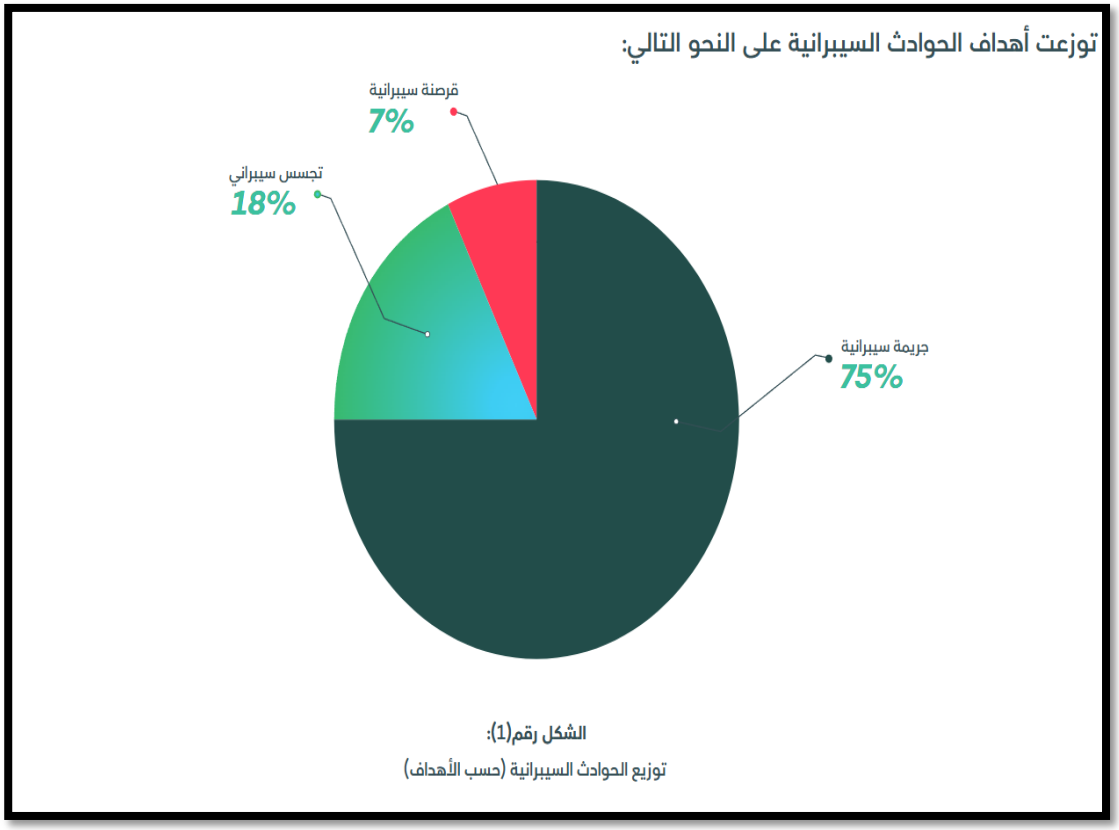
1. الاستجابة لحوادث الأمن السيبراني على المستوى الحكومي والوطني وتقديم الاستشارات وإصدار التقارير المتعلقة بها.
2. مراقبة الشبكات الحكومية وتحليل سجلات الحركات والبيانات للكشف المبكر لحالات الاختراق التي قد تتعرض لها الأنظمة والمواقع الإلكترونية الحكومية وشبكات المؤسسات الحكومية وتبليغ الجهات المعنية.

3. تحليل الأدلة الرقمية وكشف البرمجيات الخبيثة وتحديد سبب الاختراق وآليته.
4. استقبال الشكاوى والإخباريات المتعلقة بحوادث الأمن السيبراني.
5. تطوير الأطر التنظيمية لحوكمة وإدارة مخاطر الأمن السيبراني على المستوى الوطني.
6. تطوير وتطبيق السياسات في مجال الأمن السيبراني.
7. ورش عمل حول الأمن السيبراني لمختلف فئات المجتمع من مؤسسات وأفراد.
8. دورات تدريبية للأفراد والمؤسسات.
9. مسابقات أمن معلوماتي وسيبراني لطلبة المدارس والجامعات.
10. نشرات ونصائح أمنية للأفراد حول الأمن المعلوماتي.

ثالثاً. احصائيات الحوادث التي تعرضت لها الشبكات الحكومية والوطنية: بلغ عدد الحوادث السيبرانية التي تعامل معها المركز خلال سنة (2024) (3582) حادث استهدفت عدد من الوزارات والمؤسسات الحكومية فضلا عن عدد من المؤسسات الحيوية.

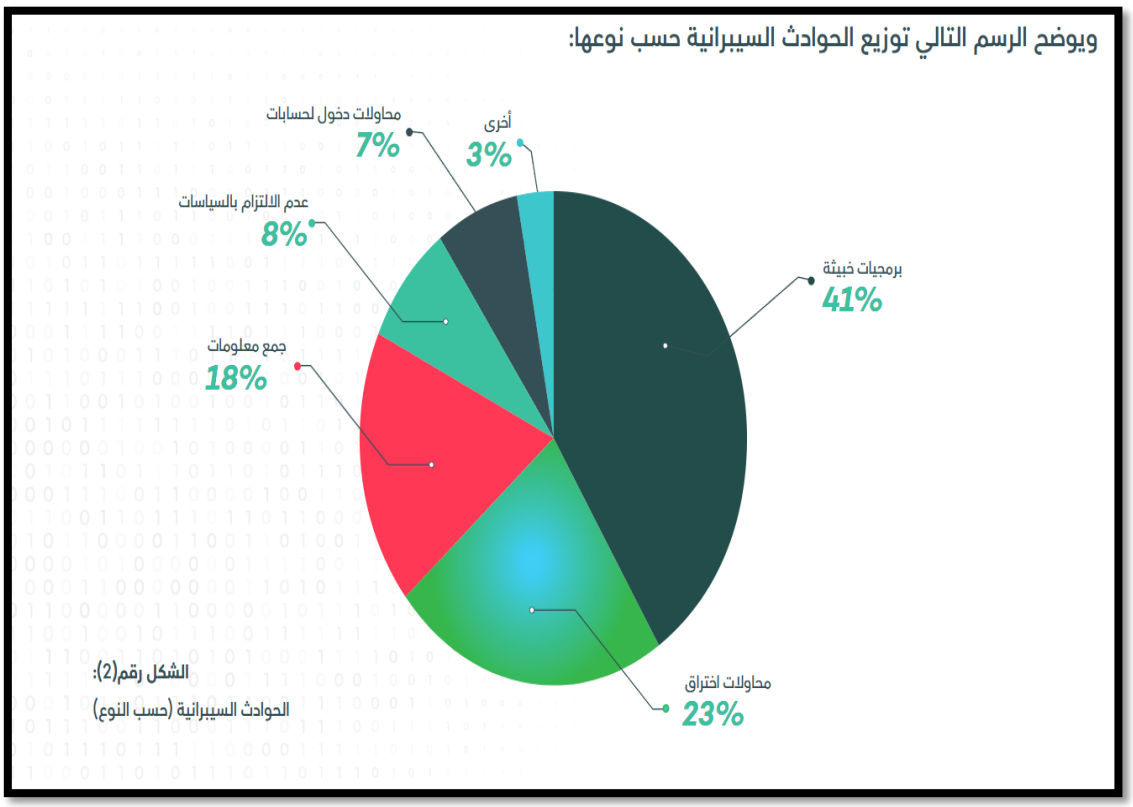
حيث لوحظ انخفاض عدد الحوادث السيبرانية المكتشفة بنسبة (23%) مقارنة بعام 2023 ويرجع السبب إلى زيادة التزام المؤسسات بتطبيق السياسات والتدابير الأمنية إلا أن الاتجاه العام للحوادث لا زال مرتفعا مقارنة بالسنوات السابقة على الرغم من انخفاضه لعام 2024.

يشير مصطلح الجريمة السيبرانية الى الأفعال غير القانونية التي يتم ارتكابها باستخدام أجهزة الكومبيوتر او الانترنت مثل سرقة البيانات، المطالبة بدفع المال، تثبيت برمجيات خبيثة واختراق الأجهزة بشكل عام.

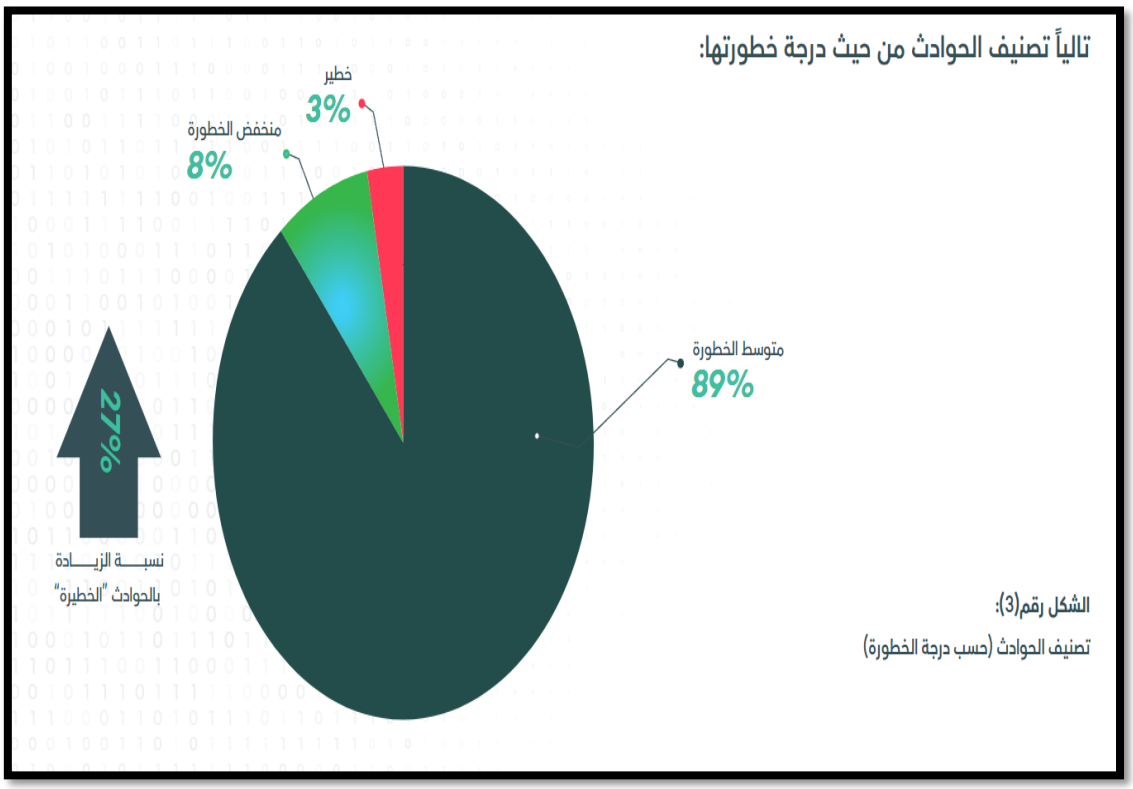


الشكل رقم(1):
توزيع الحوادث السيبرانية (حسب الأهداف)

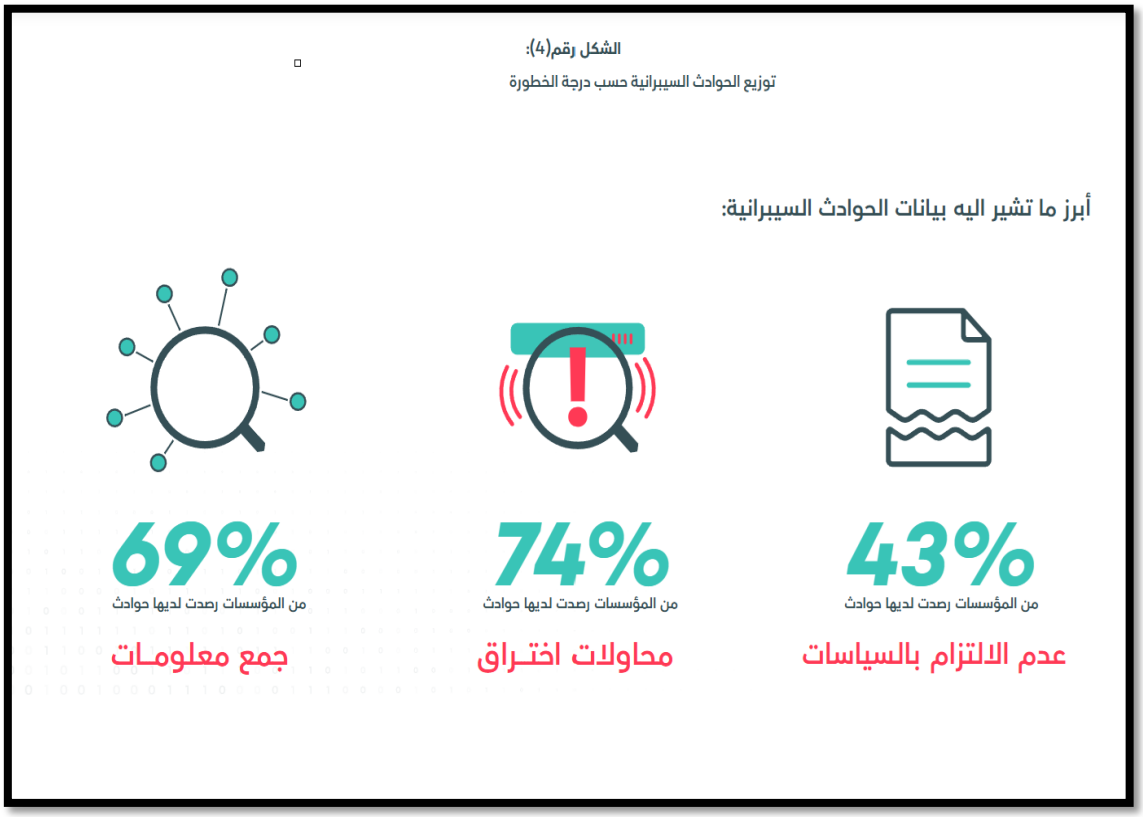
المصدر: تقارير المركز الوطني للأمن السيبراني لعام 2024



المصدر: تقارير المركز الوطني للأمن السيبراني لعام 2024



المصدر: تقارير المركز الوطني للأمن السيبراني لعام 2024.



المصدر: تقارير المركز الوطني للأمن السيبراني لعام 2024.

ثالثا. علاقات التأثير: تنص الفرضية الرئيسة على وجود تأثير معنوي للمرونة السيبرانية في تحقيق جودة الخدمات المالية. وأظهرت نتائج اختبار هذه الفرضية، كما هو موضح في الجدول رقم (1)، تحليل التباين بين المتغيرات استنادًا إلى المؤشرات التي تدل على وجود العلاقة.

جدول (1) تحليل التباين (ANOVA) للعلاقة بين المرونة السيبرانية وجودة الخدمات المالية

Model	Sum of square	DF	Mean S.	F-Value	P-Value
Reg.	15.358	1	15.358	402.862	0.000
Res.	3.457	75	0.22		
T	20.813	76			

من إعداد الباحثين استنادًا إلى مخرجات الحاسبة الإلكترونية.

ويوضح الجدول رقم (2) معاملات النموذج

جدول (2): معاملات انموذج

Model	Un. Coefficients		St. Coefficients		P-Value
	B	Std. Error	Beta	T	
Cons.	0.619	0.284		4.376	0.000
X	0.820	0.034	0.872	14.762	0.000

من إعداد الباحثين استنادًا إلى مخرجات الحاسبة الإلكترونية.

جدول (3): يحتوي على خلاصة المؤشرات التحليلية لأثر المرونة السيبرانية في أبعاد جودة الخدمات المالية

ابعاد جودة الخدمات المالية الرقمية	المؤشرات	المرونة السيبرانية	مستوى الدلالة
الوصول ودعم الزبائن	F	234.67	0.05
	P value	0.000	
	R2	0.540	
	B	0.735	
الاستخدام	F	243.675	0.05
	P value	0.000	
	R2	0.401	
	B	0.634	
جودة البيانات	F	251.18	0.05
	P value	0.000	
	R2	0.646	
	B	0.804	
ابعاد جودة الخدمات المالية الرقمية مجتمعة	F	402.862	0.01
	P value	0.000	
	R2	0.758	
	B	0.872	

من إعداد الباحثين استنادًا إلى مخرجات الحاسبة الإلكترونية.

من الجدول رقم (3) أعلاه، الذي يلخص مؤشرات التحليل على مستوى الأبعاد والفرضية، يمكننا استنتاج ما يأتي:

1. أظهر الوصول ودعم الزبائن تأثيراً معنوياً على جودة الخدمات المالية، إذ بلغت القيمة المحسوبة (F) مقدارها (206.67)، وهي أعلى من القيمة الجدولية عند مستوى دلالة ($P \leq 0.05$). كما بلغت قيمة الانحدار (B) (0.735)، مما يشير إلى أن المتغير المستقل "الوصول ودعم الزبائن" يفسر حوالي (54.0%) من التغيرات في المتغير التابع "جودة الخدمات المالية"، استناداً إلى قيمة معامل التحديد ($R^2 = 0.540$).
2. أظهر الاستخدام تأثيراً معنوياً على جودة الخدمات المالية، إذ بلغت القيمة المحسوبة (F) (103.65)، وهي أعلى من القيمة الجدولية عند مستوى دلالة ($P \leq 0.05$). كما بلغت قيمة الانحدار ((B) 0.634))، مما يشير إلى أن المتغير المستقل "الاستخدام" يفسر حوالي (40.1%) من التغيرات في المتغير التابع "جودة الخدمات المالية"، استناداً إلى قيمة معامل التحديد ($R^2 = 0.401$).
3. أظهرت جودة البيانات تأثيراً معنوياً على جودة الخدمات المالية، إذ بلغت القيمة المحسوبة (F) (231.19)، وهي أعلى من القيمة الجدولية عند مستوى دلالة ($P \leq 0.05$). كما بلغت قيمة الانحدار (B) (0.804)، مما يشير إلى أن المتغير المستقل "جودة البيانات" يفسر حوالي (64.6%) من التغيرات في المتغير التابع "جودة الخدمات المالية"، استناداً إلى قيمة معامل التحديد ($R^2 = 0.646$).

4. أظهرت المرونة السيبرانية مجتمعة تأثيرات معنوية كبيرة على أبعاد جودة الخدمات المالية، إذ بلغت القيمة المحسوبة (F) (164.98)، وهي أعلى من القيمة الجدولية عند مستوى دلالة ($P \leq 0.01$). كما بلغت قيمة الانحدار (B) (0.872)، مما يشير إلى أن المتغير المستقل "المرونة السيبرانية" يفسر حوالي (77.7%) من التغيرات في المتغير التابع "جودة الخدمات المالية"، استناداً إلى قيمة معامل التحديد ($R^2 = 0.758$).

استنادًا إلى المؤشرات التحليلية في الجدول رقم (7) أعلاه، يتضح أن جميع أبعاد المرونة السيبرانية كان لها تأثير معنوي في جودة الخدمات المالية. وهذا يشير إلى قبول الفرضية الرئيسة الثانية والفرضيات المنبثقة عنها، على الرغم من تفاوت قوة التأثير بين هذه الأبعاد.

المحور الرابع: الاستنتاجات والتوصيات

أولاً. الاستنتاجات: هدفت هذه الدراسة إلى التحقيق في العلاقة بين المرونة السيبرانية وجودة الخدمات المالية الرقمية، مع التركيز على المركز الوطني للأمن السيبراني الأردني. تسلط نتائج الدراسة الضوء على العديد من الاستنتاجات الرئيسة على النحو الآتي:

1. إن المرونة السيبرانية عنصر حاسم في تقديم خدمات مالية رقمية عالية الجودة. يتيح إطار المرونة السيبرانية القوي للمؤسسات المالية الصمود في وجه الهجمات السيبرانية، وتقليل الانقطاعات، والحفاظ على سلامة وتوافر خدماتها.
2. يعد المركز الوطني للأمن السيبراني لاعباً رئيسياً في تعزيز المرونة السيبرانية داخل القطاع المالي الأردني. تساهم جهوده في تطوير وتطبيق معايير الأمن السيبراني، وإجراء تقييمات التهديدات، وتوفير خدمات الاستجابة للحوادث بشكل كبير في وضع المرونة السيبرانية العام للمؤسسات المالية.
3. القيادة القوية والحوكمة ضرورية: القيادة الفعالة وممارسات الحوكمة القوية ضرورية لبناء المرونة السيبرانية واستدامتها. إن سياسات الأمن السيبراني الواضحة، وأطر إدارة المخاطر، والتقييمات الأمنية المنتظمة ضرورية للحفاظ على مستوى عالٍ من الأمن.
4. إن تثقيف الموظفين حول التهديدات السيبرانية، وأفضل الممارسات، وإجراءات الاستجابة للحوادث أمر بالغ الأهمية. إن القوى العاملة المدربة جيدًا هي خط الدفاع الأول ضد الهجمات السيبرانية.
5. إن التعاون بين المؤسسات المالية، والمركز الوطني للأمن السيبراني، وأصحاب المصلحة الآخرين ذوي الصلة أمر ضروري لمشاركة معلومات التهديد، وأفضل الممارسات، والدروس المستفادة. إن تبادل المعلومات يمكّن المؤسسات من معالجة التهديدات والثغرات الناشئة بشكل استباقي.

ثانياً. التوصيات: بناءً على النتائج، يمكن تقديم العديد من التوصيات لتحسين المرونة السيبرانية وجودة الخدمات المالية الرقمية:

1. على المؤسسات المالية الاستثمار في تقنيات الأمن السيبراني المتطورة التي يمكنها اكتشاف التهديدات والتخفيف منها في الوقت الفعلي. ويشمل ذلك تنفيذ حلول الذكاء الاصطناعي والتعلم الآلي لتعزيز قدرات اكتشاف التهديدات
2. إن إنشاء إطار منظم للمرونة السيبرانية يمكن أن يساعد المؤسسات على معالجة نقاط الضعف بشكل منهجي. يجب أن يشمل هذا الإطار تقييم المخاطر وتخطيط الاستجابة للحوادث واستراتيجيات التعافي.
3. تعد برامج التدريب والتوعية المنتظمة للموظفين أمرًا بالغ الأهمية. يجب أن تركز هذه البرامج على التعرف على محاولات التصيد الاحتيالي وفهم سياسات حماية البيانات وتعزيز ثقافة الأمن السيبراني.

4. على المؤسسات المالية التعاون مع خبراء الأمن السيبراني والمنظمات للبقاء على اطلاع بأحدث التهديدات وأفضل الممارسات. يمكن أن يشمل هذا التعاون أيضًا تبادل معلومات التهديد لتعزيز الأمن الجماعي.
5. يمكن أن يساعد الاختبار المستمر لتدابير الأمن السيبراني من خلال المحاكاة واختبار الاختراق في تحديد نقاط الضعف. يجب على المنظمات أيضًا تحديث بروتوكولات الأمان الخاصة بها بانتظام للتكيف مع التهديدات المتطورة.

المصادر

1. Ibrahimi Ahmed Abdel Hassan, Mohsen Alaa, & Karim Nour Al-Huda. (2019). The role of Customer Knowledge Management in Achieving Perceived Quality" Analytical study in the Fifth & Fourth Stage in IBN-HAYYAN University College. magazine of college Administration& Economics for economic & administration & financial studies, 11(4).
2. Annarelli, A., & Palombi, G. (2021). Digitalization capabilities for sustainable cyber resilience: a conceptual framework. Sustainability, 13(23), 13065.
3. Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! Comparative Strategy, 12(2), 141-165.
4. Bankuoru Egala, S., Boateng, D., & Aboagye Mensah, S. (2021). To leave or retain? An interplay between quality digital banking services and customer satisfaction. International journal of bank marketing, 39(7), 1420-1445.
5. Bapat, D. (2022). Exploring the relationship between lifestyle, digital financial element and digital financial services experience. International Journal of Bank Marketing, 40(2), 297-320.
6. Bastien, D. T., & Hostager, T. J. (1988). Jazz as a process of organizational innovation. Communication Research, 15(5), 582-602.
7. Bilge, L., & Dumitraş, T. (2012, October). Before we knew it: an empirical study of zero-day attacks in the real world. In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 833-844).
8. Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience–fundamentals for a definition. In New Contributions in Information Systems and Technologies: Volume 1 (pp. 311-316). Springer International Publishing.
9. Bodeau, D., Graubart, R., Picciotto, J., & McQuaid, R. (2011). Cyber resiliency engineering framework. MTR110237, MITRECorporation.
10. Boin, A., & Van Eeten, M. J. (2013). The resilient organization. Public Management Review, 15(3), 429-445.
11. Bossong, R., & Wagner, B. (2017). A typology of cybersecurity and public-private partnerships in the context of the EU. Crime, Law and Social Change, 67, 265-288.
12. Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. International Monetary Fund.
13. Crozier, R. (2018). Maersk Had to Reinstall All IT Systems after NotPetya Infection. itNews.
14. Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. Journal of cybersecurity, 5(1), tyz013.

15. ESRB (2020, January 7), The General Board of the European Systemic Risk Board held its 36th regular meeting on 19 December 2019, Press Release, retrieved from https://www.esrb.europa.eu/news/pr/date/2020/html/esrb.pr200107~29129d5701.en.html.
16. Greenberg, A. (2019). Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers. Anchor.
17. Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H.,... & Seager, T. P. (2013). Measurable resilience for actionable policy.
18. Luo, D., Luo, M., & Lv, J. (2022). Can digital finance contribute to the promotion of financial sustainability? A financial efficiency perspective. Sustainability, 14(7), 3979.
19. NCSC (2018, February 14), Russian military 'almost certainly' responsible for destructive 2017 cyber-attack, National Cyber Security Centre, London, retrieved from https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017- cyber-attack.
20. Olenick, D. (2018). NotPetya Attack Totally Destroyed Maersk's Computer Network: Chairman. SC Media.
21. Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. Borsa istanbul review, 18(4), 329-340.
22. Petrenko, S. (2022). Cyber resilience. River Publishers.
23. Rid, T. (2012). Cyber war will not take place. Journal of strategic studies, 35(1), 5-32.
24. Rid, T., & Buchanan, B. (2015). Attributing cyber-attacks. Journal of strategic studies, 38(1-2), 4-37.
25. Ritchie, R. (2019). Maersk: Springing back from a catastrophic cyber-attack. I–Global Intelligence for Digital Leaders.
26. Sharma, H., & Díaz Andrade, A. (2023). Digital financial services and human development: current landscape and research prospects. Information Technology for Development, 29(4), 582-606.
27. The National Academies. (2012). Disaster resilience: A national imperative. The National Academies Press. doi:10.17226/13457
28. Van Eeten, M., Nieuwenhuijs, A., Luiijf, E., Klaver, M., & Cruz, E. (2011). The state and the threat of cascading failure across critical infrastructures: the implications of empirical evidence from media incident reports. Public Administration, 89(2), 381-400.
29. Yadav, D. (2023). A Framework for Implementing Data Integrity Program Enabling Mid-Size Financial Institutions to Meet United States Federal Reserve Data Quality Requirements for Model Risk Management (Doctoral dissertation, University of Arkansas at Little Rock).