Journal Of the Iraqia University (73-2) July (2025)

ISSN(Print): 1813-4521 OnLine ISSN:2663-7502
Journal Of the Iraqia University
available online at
https://iasj.rdd.edu.iq/journals/journal/view/247

اثر برامج التوعية على إدارة مخاطر الأمن السيبراني في استدامة استقرار المصارف (دراسة حالة: مصرف الرافدين العراقي)

أ. م. سيناء احمد جارالله

الجامعة العراقية / كلية التربية للبنات

The Impact of Awareness Programs on Cybersecurity Risk Management in the Sustainability of Bank Stability

(A Case Study: Al-Rafidain Bank in Iraq)

sinai.jarallah@aliraqia.edu.iq

Introduction

Today, financial institutions face increasing cybersecurity challenges, both from individuals and unknown parties. Banks are a vast repository of sensitive information related to the financial system. Cyberattacks have become more complex and sophisticated, and the banking sector is one of the most targeted sectors due to the sensitivity of the information it handles and its economic importance. Accordingly, this study seeks to explore the impact of awareness programs on cybersecurity risk management at Rafidain Bank of Iraq and determine the extent to which these programs contribute to the bank's sustainability by analyzing the effectiveness of current awareness programs and evaluating their role in enhancing the bank's ability to confront cybersecurity threats. The study also provides recommendations for improving the effectiveness of these awareness programs, which contributes to enhancing cybersecurity and the stability of the banking sector in general. This is achieved through the use of advanced awareness programs that help bank employees take preventative measures in the event of cybersecurity risks or attacks.

المقدمة

تواجه المؤسسات المالية اليوم تحديات متزايدة في مجال الأمن السيبراني، سواء من الافراد او من جهات مجهولة كون المصارف تعد مستودع هائل للمعلومات الحساسة المتعلقة بالنظام المالي، حيث أصبحت الهجمات الإلكترونية أكثر تعقيدًا وتطورًا و يعد القطاع المصرفي من أكثر القطاعات استهدافًا نظرًا لحساسية المعلومات التي يتعامل معها وأهميتها الاقتصادية.عليه تسعى هذه الدراسة إلى استكشاف تأثير برامج التوعية على إدارة مخاطر الأمن السيبراني في مصرف الرافدين العراقي، وتحديد مدى مساهمة هذه البرامج في استدامة استقرار المصرف من خلال تحليل فعالية برامج التوعية الحالية وتقييم دورها في تعزيز قدرة المصرف على مواجهة تهديدات الامن السيبراني , كما تقدم الدراسة توصيات لتحسين فعالية هذه البرامج التوعوية ، مما يسهم في تعزيز الأمن السيبراني واستقرار القطاع المصرفي بشكل عام , من خلال استخدام برامج توعوية متطورة تساعد منتسبي المصرف باتخاذ التدابير الوقائية في حال تحقق المخاطر او الهجمات الالكترونية .

المبحث الأول

منهجية الدراسة

مشكلة الدراسة

تواجه المؤسسات المالية بصورة عامة وخاصة المصارف بصورة خاصة تحديات متزايدة في مجال الأمن السيبراني نتيجة لتطور الهجمات الإلكترونية وتعقيدها، ولان الاثار المحتملة للاختراق السيبراني تنطوي على تعرض المصارف لخسائر مادية عالية وتضرر للسمعة وغيرها، حيث يبرز هنا دور

برامج التوعية كوسيلة لتعزيز وعي الموظفين بالمخاطر السيبرانية المحتملة. لكن، يبقى السؤال حول مدى فعالية هذه البرامج التوعوية في تحسين إدارة مخاطر الأمن السيبراني في مصرف الرافدين العراقي.

اهداف الدراسة

تهدف هذه الدراسة الى التعرف على اثار تحليل فاعلية برامج التوعية الحالية في مصرف الرافدين وتحديد نقاط الضعف والقوة فيها، وتقييم دور هذه البرامج في تعزيز قدرة المصرف على مواجهة اختراقات الامن السيبراني وتقديم التوصيات لتحسين فاعلية هذه البرامج بناءً على النتائج المستخلصة من الدراسة ومن خلال تعزيز استراتيجيات الأمن السيبراني للمصرف ومساعدة صانعي على تطوير استراتيجيات أكثر فاعلية لمواجهة التحديات الأمنية المعاصرة.

أهمية الدراسة

تكمن أهمية هذا البحث كونها محاولة علمية حديثة في تقديم تحليل عميق حول تأثير برامج التوعية على إدارة مخاطر الأمن السيبراني في القطاع المصرفي، من خلال سد الفجوة المعرفية حول كيفية تحسين برامج التوعية لتكون أكثر فعالية في مواجهة تهديدات الامن السيبراني و تعزيز استقرار وأمان المؤسسات المالية بشكل عام والمصارف بشكل خاص , مما يضمن حماية المعلومات الحساسة والمحافظة على الثقة والمكانة الاقتصادية.

فرضيات الدراسة

يمكن صياغة الفرضيات بالاعتماد على المشكلة والاهداف والتي هي :

١-الفرضية الأولى:

- **H1 يوجد اثر ذو دلالة إحصائية عند مستوى معنوي (α=0.05) بين برامج التوعية وزيادة وعي الموظفين بالمخاطر السيبرانية في مصرف الرافدين.**

٢- الفرضية الثانية

- **H٢: يوجد اثر ذو دلالة إحصائية عند مستوى معنوي (α=0.05) بين تحسين برامج التوعية و عدد الحوادث السيبرانية التي يتعرض لها مصرف الرافدين .**

الدراسات السابقة

١- دراسة (٢٠١٩, محمد إسماعيل)الأمن السيبراني في القطاع المصرفي عرض مقارن للمعايير والتجارب الدولية والعربيةهدفت هذه الدراسة الى أهمية وجود معايير محددة لتنظم المخاطر السيبرانية إضافة إلى أن إدراج المخاطر السيبرانية ضمن المخاطر التشغيلية للمؤسسات المالية يعتبر غير كافي، حيث إن المعايير الرقابية على المصارف تتطلب أهمية تضمين الاستراتيجيات والسياسات الخاصة بتلك من قبل مجالس إدارات البنوك مع زيادة حجم المخاطر السيبرانية , كما اكدت على الإطار الرقابي العام للمخاطر المرتبطة بأمن نظم المعلومات والفضاء الإليكتروني من خلال وجود توجيهات رقابية تلزم المصارف بتضمين استراتيجيات المخاطر مقرة من قبل مجالس إدارات البنوك إطاراً يتعلق بالمخاطر الإلكترونية ومخاطر نظم المعلومات والهجمات الإلكترونية attacks)

دراسة(٢٠٢١, مروه فتحي السيد)

اقتصاديات الأمن السيبراني في القطاع المصرفي تعتبر الصيرفة الإلكترونية جانبا هاما من جوانب التجديد في القطاع المصرفي، في خضم عديد التحديات التي يفرضها الاندماج في الاقتصاد العالمي على هذا القطاع الاقتصادي الهام، خصوصا و أن من أبرز ملامح المرحلة الراهنة المنافسة الشديدة المستفيدة من آخر ثمار تكنولوجيا الإعلام و الاتصال، قد طرأت على الساحة المصرفية تغيرات متلاحقة و بإيقاع متسارع على نحو بات معه الشكل التقليدي للبنوك محل تهديد من خلال المخاطر السيبرانية ومدى أهمية تعزيز قدرة الأجهزة المصرفية على تحمل هذه المخاطر والتحوط منها، فقد اتخذت السلطات الرقابية على مستوى العالم خطوات تنظيمية وإشرافية تهدف إلى تجنب أثر تلك المخاطر السيبرانية على المصارف.

٣- **دراسة (Eisenbach,Lee .٢٠٢٢)**هدفت هذه الدراسة الى توضيح كيف يمكن ان تشن الهجمات السيبرانية على مصرف واحد او عدة مصارف من خلال أنظمة عدة ومنها نظام المدفوعات , حيث من المرجح ان يتم تضخيم أي هجوم على اكثر البنوك الامريكية نشاطا والذي يضعف من قدرات تلك البنوك على ارسال المدفوعات للتاثير على السيولة في العديد من البنوك الأخرى ,وقد يكون في المناطق الجغرافية ذات البنوك المركزية الأكبر .

حدود الدراسة

تتمثل الحدود المكانية لهذه الدراسة في مصرف الرافدين، بما يشمل بعض من فروعه المنتشرة في بغداد.

الحدود الزمانية

شملت الفترة الزمنية المحددة للدراسة، والتي كانت ثلاثة أشهر، وذلك بحسب طبيعة هذه الدراسة والتي كانت دراسة ميدانية شملت مصارف الرافدين بأغلب فروعها في بغداد.

الحدود الموضوعية

تركز الدراسة على موضوع محدد مثل تأثير برامج التوعية على إدارة مخاطر الامن السيبراني لضمان استدامة واستقرار المصرف.

الحدود البشرية

تشمل العينة البشرية التي تم اختيارها للدراسة مثل المدراء العامون، مدراء الفروع، مدراء الدوائر المالية، مدراء إدارة الخطر في المصرف، موظفي المصرف، أي فئات أخرى ذات صلة بموضوع الدراسة.

المبحث الثاني

الإطار الفكري

الأمن السيبراني في القطاع المصرفي

تعتبر المصارف هدفا رئيسيا لهجمات الحوادث السيبرانية, كما تشكل تهديدا كبيرا للنظام المالي حيث تشير التقارير والبيانات الى ان الهجمات الالكترونية التي تشن على المصارف أدت الى سرقة مليارات الدنانير , وان عملية اختراق هذه المصارف اصبح حالة ليست بالمستحيلة في يومنا هذا بسبب التقدم الحاصل في المجال الالكتروني والعولمة المتزايدة والاستخدام المزمن للتكنلوجيا المتقدمة و الترابط الكبير والسريع الحاصل بين النظام المالي والبنى التحتية لتكنلوجيا المعلومات , والطبيعة الحساسة لأعمال وخدمات المؤسسات المالية بصورة عامة والمصارف بصورة خاصة كما تعتبر المصارف أهدافا جذابة لمجرمي الانترنت والاختراقات الالكترونية كما ان انتشار الخدمات المصرفية المتقدمة وبسبب الجهل وقلة المعرفة من قبل العملاء يكون هناك تفاقم لهذه التهديدات و الهجمات الالكترونية , وتعتبر مخاطر الامن السيبراني شكلا من اشكال المخاطر ذات الخسارة الناتجة عن الحوادث الرقمية الداخلية والخارجية والتي بما فيها السرقة والاحتيال والتلف وتعطيل الاعمال , وقد تؤدي حوادث مخاطرا امن السيبراني الى اضعاف سرية وسلامة وتوفير البيانات والمعلومات , حيث ان أنظمة الامن السيبراني هي أنظمة مدعمة بالذكاء الاصطناعي لحماية المصارف من الاختراقات والانتهاكات المحتملة التحقق ومنعها واتخاذ اللازم في حال تحققها , لدعم العملاء وتوفير الخدمات المصرفية باعلى جودة من خلال اتمتة العمليات المصرفية.وعليه يمكن تعريف مخاطر الامن السيبراني على انها المخاطر التشغيلية لاصول المعلومات التي تؤثر على سرية وسلامة المعلومات او أنظمة المعلومات. , كما يمكن تعريف الامن السيبراني على انه هو ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية. تهدف هذه الهجمات عادة إلى الوصول إلى المعلومات الحساسة أو تغييرها أو تدميرها، بهدف الابتزاز المالي من المستخدمين أو مقاطعة العمليات التجارية.

أنواع مخاطر الأمن السيبراني في المصارفيمكن تصنيف مخاطر الامن السيبراني الى عدة أنواع من الهجمات الإلكترونية مثل هجمات البرمجيات الخبيثة(Malware) ، وهجمات الفدية (Ransomware) التي تستهدف الأنظمة لشل حركت العمليات المصرفية أو سرقة البيانات العملاء والتي نذكر منها :-

١. **التصيد الاحتيالي** حيث يتم خداع العملاء من خلال رسائل بريد إلكتروني أو مواقع مزيفة تبدو من مصدر موثوق للكشف عن معلومات حساسة مثل أسماء المستخدمين وكلمات المرور.

٢. **اختراق البيانات** :يستهدف هذا النوع من المخاطر سرقة البيانات الحساسة للعملاء مثل الأرقام السرية لحساباتهم أو معلومات بطاقاتهم الائتمانية.

٣. **الهجمات الموزعة لحجب الخدمة** تهدف هذه الهجمات إلى إغراق الشبكة أو السيرفرات بالطلبات الزائفة لجعل النظام غير قادر على تلبية الطلبات المشروعة وتعطيل الخدمات المصرفية وغالبا ما يكون من خلال استخدام اجهزه مخترقة .

مخاطر الأمن السيبراني في الخدمات المصرفيةتعتبر الخدمات المصرفية من القطاعات الحيوية التي تعتمد بشكل كبير على التكنولوجيا الرقمية لتقديم خدماتها. ومع تطور العالم الرقمي والاعتماد المتزايد على التكنولوجيا، يواجه القطاع المصرفي مجموعة من التحديات والمخاطر المتعلقة بالأمن السيبراني من خلال البرمجيات الخبيثة مثل الفيروسات المستخدمة من قبل هكرات الانترنت لاستهداف الأنظمة المصرفية والتي تُسبب سرقة

البيانات أو تعطيل العمليات المصرفية من خلال البرمجيات التي تدخل إلى الأنظمة عبر الروابط المشبوهة أو المرفقات الضارة في البريد الإلكتروني, وكذلك يعد الاحتيال الإلكتروني من أكبر المخاطر التي تواجهها المصارف كل هذا يؤدي الى اختراقات البيانات الحساسة و الخاصة بالعملاء مثل أرقام الحسابات وكلمات المرور مما يتسبب في خسائر مالية فادحة وفقدان الثقة بين العملاء والمصرف.

التوعية بالمخاطر السيبرانية في المصارفتعرف التوعية بالمخاطر السيبرانية هي عملية تهدف إلى تثقيف الأفراد والمؤسسات بصورة عامة والمصارف بصورة خاصة حول التهديدات الإلكترونية وكيفية التصدي لها, حيث تشمل هذه العملية تعليم أفضل الممارسات للأمن السيبراني، مثل تحديد رسائل البريد الإلكتروني الاحتيالية، واستخدام كلمات مرور قوية، وتحديث البرامج بانتظام، بالإضافة إلى تعزيز السلوكيات الآمنة عبر الإنترنت والهدف الرئيسي هو تقليل المخاطر التي تتعرض لها البيانات والأنظمة من خلال زيادة الوعي والمعرفة حول كيفية حماية المعلومات الحساسة من التهديدات السيبرانية.حيث تساهم برامج التوعية في تعزيز أمن المعلومات في المؤسسات المالية والمصارف من خلال برامج التوعية التي تساهم بشكل كبير في تعزيز أمن المعلومات ومن خلال عدة طرق:

١. **زيادة الوعي بالمخاطر:**

حيث تساعد برامج التوعية للمنتسبين من خلال فهم التهديدات المحتملة التي قد تحدث مثل التصيد الاحتيالي والهجمات الإلكترونية وغيرها من التهديدات ، مما يعزز قدرت هؤلاء المنتسبين على التعرف عليها وتجنبها.

٢. **تعزيز الثقافة الأمنية:**تدريب موظفي المصارف على برامج إدارة مخاطر الامن السيبراني والتي تساعدهم على بناء ثقافة أمنية قوية داخل المصرف، والتي تصبح جزءًا من السلوك اليومي للموظفين.

٣. **تدريب الموظفين على أفضل الممارسات:**تقدم برامج التوعوية والإرشادية حول السياسات والإجراءات الأمنية المناسبة، مثل كيفية إنشاء كلمات مرور قوية، وتحديث البرامج بانتظام، والتعامل بحذر مع البريد الإلكتروني.وعليه تلعب برامج التوعية دورًا حيويًا في تقوية دفاعات المصارف ضد تهديدات الامن السيبراني، مما يحافظ على سلامة البيانات المالية وحماية ثقة العملاء من خلال عدة عناصر أساسية تهدف إلى تعزيز معرفة الموظفين وتقوية دفاعات المصرف ضد التهديدات السيبرانية والتي تشمل التدريب العملي من خلال تقديم دورات تدريبية تفاعلية تتضمن أمثلة واقعية ومواقف عملية تساعد الموظفين على تطبيق ما تعلموه في بيئة العمل اليومية , وكذلك تنظيم ورش عمل منتظمة تجمع بين التوعية النظرية والتطبيقية، إضافة الى التحديثات الدورية حيث توفر تحديثات مستمرة حول أحدث التهديدات السيبرانية والتقنيات الدفاعية التي قد يتعرض لها المصرف ، لضمان أن الموظفين على اطلاع دائم بالمستجدات , وكذلك توعية العملاء عبر البريد الإلكتروني والنشرات الإخبارية من خلال إرسال رسائل بريد إلكتروني أو نشرات إخبارية للعملاء تحتوي على نصائح أمنية، وتحذيرات من التهديدات الجديدة.

برامج توعية إدارة مخاطر الأمن السيبرانيتعد برامج توعية إدارة مخاطر الأمن السيبراني تلعب دورًا حاسمًا في حماية الأفراد والمنظمات من التهديدات المتزايدة في الفضاء الإلكتروني والتي منها التعرف على الهجمات السيبرانية من خلال كيفية التعرف على رسائل البريد الإلكتروني الاحتيالية ومؤشرات البرامج الضارة والفيروسات، وكذلك التدريب على الممارسات الآمنة لاستخدام الإنترنت، من خلال أهمية استخدام كلمات مرور قوية وفريدة لتجنب الثغرات الأمنية من خلال:

١- سياسات الشركة المتعلقة بالأمن السيبراني.

٢-معرفة الإجراءات اللازمة في حال وقوع خرق أمني.

٣-التعامل مع البيانات الشخصية والحساسة.

٤-حماية بيانات المصرف.

٥-حماية بيانات العملاء.حيث تهدف هذه البرامج إلى تعزيز الوعي والفهم بين الموظفين والمستخدمين لضمان أن يكون لدى الجميع القدرة على التعرف على اخطار الامن السيبراني المحتملة واتخاذ الإجراءات الوقائية المناسبة.

المبحث الثالث الدراسة الميدانية

يركز هذا الجزء من الدراسة على اثر برامج التوعية على إدارة مخاطر الأمن السيبراني في استدامة استقرار المصارف، حيث تم تصميم هذه الدراسة والتجربة بعناية لضمان الحصول على بيانات دقيقة وموثوقة, حيث يهدف الجانب العملي إلى اختبار الفرضيات المطروحة وتقديم حلول عملية قابلة للتنفيذ, من خلال هذه الدراسة، ومن خلاله نطمح إلى تقديم إضافة قيمة للمجال العلمي وفتح آفاق جديدة للبحوث المستقبلية والتطبيقات العملية.حيث تم استخدام برنامج SPSS لتحليل البيانات وتفريغ استمارات الاستبيان حيث كان عدد مجتمع الدراسة (١٣٠) من مدراء عامين، مدراء

فروع، موظفين ادارة المخاطر ومحاسبين في مصرف الرافدين، حيث تم توزيع الاستبانات وتم استرجاع ١٢٠ استمارة فقط وكانت ١٠ استمارات غير صالحة او لم تعاد وكانت على النحو التالي: **الجدول رقم (١) البيانات الديمغرافية**

المتغير	البيان	العدد	النسبة
المسمى الوظيفي	مدير عام	١٣	٪١١
	مدير فرع	٢٢	٪١٨
	موظف	٣٧	٪٣١
	محاسب	٤٨	٪٤٠
	المجموع	١٢٠	٪١٠٠
المؤهل العلمي	اعدادية	٣٥	٪٢٩
	دبلوم	١٢	٪١٠
	بكلوريوس	٥٨	٪٤٨
	ماجستير	١٥	٪١٣
	المجموع	١٢٠	٪١٠٠
سنوات الخبرة	اقل من ٥ سنوات	٣١	٪٢٥
	من ٥ الى ١٠	٤٧	٪٤٠
	من ١١الى ١٥ سنة	١٩	٪١٦
	اكثر من ١٥ سنة	٢٣	٪١٩
	المجموع	١٢٠	٪١٠٠

فيما يخص الجزء الأول حيث تم تقسيم الجدول الى ثلاثة فقرات حيث كانت الفقرة الأولى للمسمى الوظيفي (مدير عام، مدير فرع، موظف، محاسب) حيث كانت اعلى نسبة لفئة المحاسبين والذي كانت نسبتهم (٤٠٪) وعددهم (٤٨) من اصل عينة الدراسة، اما فيما يخص المؤهل العلمي (اعدادية، دبلوم، بكلوريوس , ماجستير) فقد كانت اعلى نسبة لشهادة البكلوريوس والتي كانت نسبتهم (٥٨) وبنسبة (٤٨٪) , وأخيرا فقرة سنوات الخبرة والتي كانت اعلى نسبة (٤٠٪) لفئة العاملين الذين لديهم خدمة تتراوح بين (٥-١٠) سنوات وكان عددهم (٤٧) موظف من اصل العينة اما بخصوص الجزء الثاني من الاستبانة والذي كان يخص برامج التوعية على إدارة المخاطر السيبرانية في استدامة استقرار المصارف حيث تم تقسيمها الى ثلاثة محاور من خلال الاعتماد على مقياس ليكرت الخماسي وكما موضح في الجداول ادناه **الجدول رقم (٢) مقياس لكرت الخماسي**

التصنيف	موافق بدرجة كبيره جدا	موافق بدرجة كبيرة	محايد	غير موافق	غير موافق بدرجة كبيرة
الدرجة	٥	٤	٣	٢	١

٣-١- اختبار ثبات وصدق أداة الدراسة لغرض التأكد من موثوقية أداة الدراسة المستخدمة وثبات الدراسة والتي تعكس ثبات أداة القياس , فقد تم احتساب معامل الثبات والتي كانت قيمتها (٨٦) وبحسب معامل الثبات كرونباخ, والتي تمثل نسبة عالية تؤكد ثبات الأداة للبحث وعليه فأنها صالحة للتحليل الاحصائي وبالإمكان الاعتماد على نتائجها بدرجة عالية .

٣-٢- نتائج اختبار الفرضية الأولى

H1 : يوجد اثر ذو دلالة إحصائية عند مستوى معنوي (α=0.05) بين برامج التوعية وزيادة وعي الموظفين بالمخاطر السيبرانية في مصرف الرافدينوللتحقق من الفرض الأول والذي تم اختباره من خلال مجموعة أسئلة تم توجيها الى من يهمه الامن باستبانة موزعة على عدد من المعنين في مصرف الرافدين، والتي تتعلق برامج التوعية وأثرها على زيادة وعي الموظفين بالمخاطر السيبرانية وبحسب ما موضح ادناه: الجدول رقم (٣)

	تساهم النتائج المتحققة في تبني برامج التوعية على زيادة وعي الموظفين بالمخاطر السيبرانية وحسب.	الوسط الحسابي	الانحراف المعياري	قيمة T
١	للموظف معرفة كافية بمخاطر الامن السيبراني التي قد يتعرض لها المصرف خلال أعماله اليومية .	٢.٥٤٥	٠.٢٣٤	57.32
٢	هل للموظف القدرة على التعرف على التهديدات السيبرانية الشائعة في المصارف ؟	2.382	0.393	63.67
٣	تعد برامج التوعية الحالية المقدمة في مجال الامن السيبراني في المصرف كافية ومفيدة ؟	5.346	0.510	67.22
٤	هل تؤيد دعم إدارة المصرف للمشاركة في برامج التوعية الخاصة بالأمن السيبراني؟	3.049	0.503	56.45
٥	هل ترى أن هناك تحسنًا ملموسًا في تعامل الموظفين مع إدارة مخاطر الامن السيبراني بعد برامج التوعية؟	4.753	0.480	76.43
٦	هل تساهم البرامج التوعوية في تقليل حوادث الامن السيبراني بالمصرف؟	4.127	0.436	77.12
٧	هل اختلفت معرفتك بمفاهيم إدارة مخاطر الأمن السيبراني قبل وبعد الالتحاق ببرامج التوعوية التي تخص إدارة مخاطر الامن السيبراني ؟	3.209	0.358	50.67
٨	هل محتوى وجودة البرامج التوعوية المقدمة للموظفين بالمستوى المطلوب ؟	4.296	0.832	57.93
٩	هل تشعر بالثقة في التعامل مع حوادث الأمن السيبراني بعد حضور برامج التوعية الخاصة بإدارة المخاطر السيبرنية؟	3.223	0.313	79.32
١٠	هل تأثير برامج التوعية في تغيير سلوك الموظفين تجاه اتباع إجراءات الأمان السيبراني أصبحت افضل بعد تقديم البرامج التوعوية ؟	4.575	0.504	78.76
	الإجمالي المتوسط	**3.750**	**0.456**	**66.489**

نستنتج من الجدول رقم (٣) والمتضمن تحليل البيانات الخاصة باختبار الفرضية الأولى والتي تشمل تحليل الأسئلة الموجه للمعنيين تبين ان المتوسط الحسابي لإجابات العينة تتراوح بين (5.346) والتي هي الحد الأعلى والتي تنص على ان برامج التوعية الحالية المقدمة في مجال الامن السيبراني في المصرف كافية ومفيدة , وبين (2.382) والتي هي الحد الأدنى حيث يرجع انخفاض الوسط الحسابي الى السؤال الذي

نصه للموظف معرفة كافية بمخاطر الامن السيبراني التي قد يتعرض لها المصرف خلال أعماله اليومية كما ان اجمال المتوسط الحسابي لجميع الأسئلة والتي كانت النسبة **(3.750)** وهو رقم مرتفع وبانحراف معياري **(0.456)** وكان متوسط قيمة T (**66.489**) كل هذه النسب اكتدت على ان تبني البرامج التوعوية من قبل المصرف تساعد على زيادة وعي الموظفين بمخاطر الامن السيبراني.

٣-٣- نتائج اختبار الفرضية الثانية

٢- الفرضية الثانية

• **H٢: يوجد اثر ذو دلالة إحصائية عند مستوى معنوي (α=0.05) بين تحسين برامج التوعية و عدد الحوادث السيبرانية التي يتعرض لها مصرف الرافدين** حيث تم اختبار هذه الفرض من خلال الأسئلة الموجه لعينة الدراسة وتم التوصل للنسب المذكرة ادناه والتي تتعلق بقياس مساهمة النتائج المتحققة من أثر برامج التوعية وعدد الحوادث السيبرانية التي يتعرض لها مصرف الرافدين، وكانت النتائج الإحصائية كما يلي:الجدول رقم (٤)

	يوجد اثر ذو دلالة إحصائية عند مستوى معنوي (α=0.05) بين تحسين برامج التوعية و عدد الحوادث السيبرانية التي يتعرض لها مصرف الرافدين .	الوسط الحسابي	الانحراف المعياري	قيمة T
١	يعمل مصرف الرافدين باستمرار على تطوير وتحديث البرامج التوعوية لكيفية إدارة مخاطر الامن السيبراني ؟	5.188	0.399	62.96
٢	يعتمد مصرف الرافدين على الوسائل الحديثة في تطوير مهارات الموظفين لمواجهة هجمات مخاطر الامن السيبراني على المصرف ؟	3.915	0.793	88.32
٣	يقدم المصرف برامج توعية مكثفة لحماية الخدمات المالية كونها الأكثر تعرضا لهجمات مخاطر الامن السيبراني ؟	2.913	0.579	83.15
٤	يتخذ المصرف دائما خطوات استباقية من خلال دورات توعوية لمواجهة مخاطر الامن السيبراني ؟	2.797	0.705	91.18
٥	يعتمد المصرف المعايير الدولية في التوعية للتحوط من مخاطر الامن السيبراني ؟	3.573	0.291	69.28
٦	يوفر المصرف قنوات واضحة للإبلاغ عن أي حوادث سيبرانية مشتبه بها بعد تقديم برامج التوعية؟	4.975	0.795	91.94
٧	يشجع المصرف على ثقافة الأمن السيبراني كجزء من القيم المؤسسية المعتمدة ضمن برنامج التوعية؟	2.838	0.499	85.62
٨	تحتوي برنامج التوعية في المصرف على تدريبات عملية تساعد الموظفين على اكتساب مهارات التعامل مع مخاطر هجمات الامن السيبراني؟	5.918	0.637	59.31
٩	تساهم البرامج التوعوية في مجال إدارة مخاطر الامن السيبراني في تقليل مخاطر الهجمات الالكترونية ؟	3.329	0.479	92.04
١٠	هل يتم تقييم فعالية برامج التوعية بشكل دوري لضمان تحسينها ومواكبتها للتطورات في مجال إدارة مخاطر الأمن السيبراني؟	4.989	0.714	80.50
	متوسط الإجمالي	**4.043**	**0.589**	٨٠.٤٣

نستنتج من الجدول رقم (٤) والمتضمن تحليل البيانات الخاصة باختبار الفرضية الثانية والتي تشمل تحليل الأسئلة الموجه للمعنيين تبين ان المتوسط الحسابي لإجابات العينة تتراوح بين **(5.918)** والتي هي الحد الأعلى والتي تنص على ان تحتوي برنامج التوعية في المصرف على تدريبات عملية تساعد الموظفين على اكتساب مهارات التعامل مع مخاطر هجمات الامن السيبراني , وبين (2.797) والتي هي الحد الأدنى حيث يرجع انخفاض الوسط الحسابي الى مدى مساهمة المصرف باتخاذ خطوات استباقية من خلال دورات توعوية لمواجهة مخاطر الامن السيبراني , وبمتوسط اجمالي (**4.043**) للوسط الحسابي و متوسط اجمالي للانحراف المعياري قدره (**0.589**), وكان متوسط قيمة T (٨٠.٤٣) .

المبحث الرابع

الاستنتاجات والتوصيات

٤-١ الاستنتاجات

تعد البرامج التوعوية الخاصة بمخاطر الأمن السيبراني من الأمور المهمة التي تعزيز قدرة المصرف على مواجهة التهديدات من خلال تحليل اثر هذه البرامج التوعوية على منتسبي المصرف ومدى فعاليتها في تحسين إدارة مخاطر الأمن السيبراني وضمان استدامة استقرار المصرف حيث تم التوصل الى عدة استنتاجات نذكر منها:-.

١-تعزيز الوعي من خلال البرامج التوعوية الخاصة بمخاطر الامن السيبراني والتي ساهمة بشكل كبير في زيادة وعي الموظفين بمخاطر الامن السيبراني، والتي بدورها تقلل من احتمالية حدوث الثغرات الأمنية الناتجة عن خطأ الموظف.

٢- انخفاض مخاطر الامن السيبراني بعد تحسن جودة البرامج التوعوية والتي أدت بدورها الى انخفاضًا ملحوظًا في عدد هذه الحوادث، مما يؤكد فاعلية هذه البرامج كإجراء وقائي.

٣-أسهمت برامج التوعية في مجال مخاطر الامن السيبراني في تحسين استجابة الموظفين للحوادث السيبرانية من خلال تزويدهم بالمعرفة والمهارات اللازمة للتعامل مع التهديدات بفعالية.

التوصيات

تتطلب برامج التوعية تحسينات مستمرة لضمان فعاليتها في مواجهة تهديدات مخاطر الامن السيبراني , حيث تهدف هذه التوصيات إلى تعزيز قدرة المصرف على إدارة مخاطر الأمن السيبراني بفعالية أكبر والتي نذكر منها :-

١-ضمان دعم الإدارة العليا والتزامها بتعزيز ثقافة مواجهة مخاطر الأمن السيبراني داخل المصرف من خلال مشاركتهم في ورش العمل والفعاليات ذات الصلة.

٢-تحديث محتوى البرامج التوعوية الخاصة بمخاطر الامن السيبراني من خلال مواكبة أحدث التطورات في مجال الأمن السيبراني وباستخدام الذكاء الاصطناعي.

٣-إشراك جميع الموظفين بغض النظر عن مناصبهم لضمان وجود وعي شامل ومتكامل داخل المصرف بمخاطر الامن السيبراني وكيفية التعامل مع هذه المخاطر في حال تحققها.