



أثر إدارة مخاطر العامل البشري على الحد من الهجمات السيبرانية: دراسة
ميدانية على المؤسسات الحكومية في المملكة العربية السعودية

إعداد الطالب/
وليد نبيل القباني
2021201871

إشراف/
د. الفیصل عبد الحمید محمد حسن
العام الدراسي:
2025 – 1447

المستخلص

تهدف الدراسة إلى معرفة مدى أثر تطبيق إدارة مخاطر العامل البشري بأبعادها مجمعة المتمثلة في (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد من الهجمات السيبرانية: دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية ، تم اتباع المنهج الوصفي التحليلي، تم توزيع الاستبانة على عينة عشوائية من العاملين في البنوك الحكومية بمدينة الرياض، وقد بلغ عدد الاستبانات الصالحة للتحليل (350) استبانة، استخدم الباحث مجموعة من الأساليب الإحصائية لتحليل البيانات. أظهرت نتائج الدراسة وجود مستوى مرتفع جدا من تحديد وتقييم المخاطر كأحد ابعاد إدارة مخاطر العامل البشري ، و وجود مستوى مرتفع جدا من معالجة إدارة المخاطر كأحد ابعاد إدارة مخاطر العامل البشري وفي ضوء النتائج، توصي الدراسة بتعزيز برامج التوعية الأمنية المستمرة لجميع الموظفين، مع التركيز على التهديدات السيبرانية المرتبطة بالسلوك البشري كالهندسة الاجتماعية والتصيد الإلكتروني ، تضمين إدارة مخاطر العامل البشري ضمن الخطة الاستراتيجية للأمن السيبراني في المؤسسات الحكومية لضمان معالجة التهديدات البشرية بشكل منهجي.

الكلمات المفتاحية: مخاطر العامل البشري - الهجمات السيبرانية - المؤسسات الحكومية

Abstract

The study aims to determine the impact of applying human factor risk management, with its combined dimensions (risk identification and assessment, risk management treatment, and risk management monitoring), on reducing cyberattacks: a field study on government institutions in the Kingdom of Saudi Arabia. The descriptive-analytical approach was adopted, and a questionnaire was distributed to a random sample of employees in government banks in Riyadh. The number of valid questionnaires for analysis was 350. The researcher used a set of statistical methods to analyze the data. The study results showed a very high level of risk identification and assessment as one of the dimensions of human factor risk management, as well as a very high level of risk management treatment. In light of the findings, the study recommends enhancing ongoing security awareness programs for all employees, with a focus on cyber threats related to human behavior such as social engineering and phishing. It also recommends incorporating human factor risk management into the strategic cybersecurity plan of government institutions to ensure systematic handling of human-related threats.

Keywords: Human Factor Risks – Cyberattacks – Government Institutions

المقدمة

تُعد إدارة المخاطر عنصرًا أساسيًا يلعب دورًا حيويًا في نجاح المؤسسات الحديثة، إذ تُسهم في تحقيق الأهداف الاستراتيجية وتعزيز القدرة التنافسية. تتضمن إدارة المخاطر تحديد المخاطر المحتملة وتقييمها ووضع الخطط المناسبة لمواجهتها، مما يُساعد على تقليل الآثار السلبية التي قد تؤثر على الأداء العام للمؤسسة. (سلمونة، 2024)

تبدأ عملية إدارة المخاطر بتحديد أنواع المخاطر المختلفة التي قد تواجهها المؤسسة، سواءً كانت مالية أو تشغيلية أو استراتيجية أو حتى بيئية. ومن خلال هذه العملية، يُمكن للمؤسسات توقع التحديات المحتملة ووضع استراتيجيات فعالة للتخفيف من آثارها. على سبيل المثال، قد تشمل المخاطر المالية تقلبات السوق أو تغيرات أسعار المواد الخام، بينما قد تشمل المخاطر التشغيلية مشاكل سلسلة التوريد أو عدم الكفاءة التشغيلية. (العنبرية، 2023)

بعد تحديد المخاطر، تأتي المرحلة التالية وهي تقييمها. يتطلب ذلك تحليل مدى تأثير كل خطر على المؤسسة واحتمالية حدوثه. يُساعد هذا التحليل على تخصيص الموارد بفعالية أكبر، حيث يُمكن للمؤسسات التركيز على المخاطر الأكثر تأثيرًا واحتمالية، مما يُعزز فعالية استراتيجيات التخفيف من آثارها. تتطلب إدارة المخاطر أيضًا توعية الموظفين وتثقيفهم، إذ يلعب كل فرد داخل المؤسسة دورًا في تحديد المخاطر والاستجابة لها على النحو المناسب. ومن خلال بناء ثقافة مؤسسية تُعزز أهمية إدارة المخاطر، يُمكن للمؤسسات المساهمة في تعزيز المرونة والقدرة على الاستجابة السريعة للتغيرات والضغوط الخارجية. (القحطاني، 2023)

إدارة المخاطر ليست مجرد عملية روتينية، بل هي عنصر أساسي لاستدامة الأعمال ونجاحها في بيئة عمل معقدة ومتغيرة باستمرار. ومن خلال استراتيجيات فعالة لإدارة المخاطر، لا تستطيع المؤسسات حماية نفسها من التهديدات فحسب، بل أيضًا اغتنام فرص جديدة للنمو والتوسع. (المري، 2020)

يُعد العامل البشري أحد أهم العناصر في أي مؤسسة، إذ يلعب دورًا حيويًا في تشكيل نجاحها وفعاليتها. فالموظفون ليسوا مجرد أدوات تشغيلية، بل هم المحرك الرئيسي الذي يُسهم في تحقيق الأهداف الاستراتيجية للمؤسسة. ويتجلى تأثير العامل البشري في جوانب عديدة، منها الإبداع والتفاعل والتكيف مع التغيير، مما يُسهم بشكل مباشر في تحسين الأداء العام للمؤسسة. (باقر، 2020)

ومن الجوانب الأساسية لتأثير العامل البشري القدرة على الإبداع والابتكار. فالأفراد ذوو المهارات والخلفيات الثقافية المتنوعة قادرون على تقديم أفكار جديدة وحلول مبتكرة للمشكلات. وهذا التنوع في التفكير يُعزز قدرة المؤسسة على المنافسة في الأسواق المتغيرة، ويُساهم في تطوير منتجات وخدمات جديدة تُلبّي احتياجات العملاء بشكل أفضل. لذلك، يُصبح الاستثمار في تطوير مهارات الموظفين وتعزيز ثقافة الابتكار أمرًا أساسيًا لضمان استمرار النجاح. (الحسني، 2022)

علاوة على ذلك، يلعب التفاعل الشخصي داخل مكان العمل دورًا محوريًا في تعزيز التواصل والتعاون. فعندما يتمتع الموظفون ببيئة عمل تُشجع على المشاركة الفعالة وتبادل الأفكار، يُسهم ذلك في بناء علاقات قوية تُعزز روح الفريق. تساعد هذه الروح التعاونية على تحسين الكفاءة وتقليل الأخطاء، حيث يعمل الأفراد معًا لتحقيق أهداف مشتركة. كما يعكس تعزيز العلاقات الإنسانية في العمل التزام المؤسسة برفاهية موظفيها، مما يؤثر إيجابًا على الإنتاجية والرضا الوظيفي. (الرواشدة، 2022)

تُعد القدرة على التكيف مع التغيير عاملاً بشرياً مهماً أيضاً. ففي عالم سريع التغير، تحتاج المؤسسات إلى أفراد قادرين على مواجهة التحديات الجديدة والتكيف مع الظروف المتغيرة. فالموظفون الذين يتمتعون بالمرونة العقلية والقدرة على التعلم السريع قادرون على الاستجابة بفعالية للابتكارات التكنولوجية وتقلبات الأسواق. ولا يقتصر هذا التكيف على الحفاظ على استقرار المؤسسة فحسب، بل يعزز أيضاً قدرتها على استكشاف فرص جديدة. (أبو نصر، 2020)

لا يمكن الاستهانة بأهمية العامل البشري في تحقيق النجاح المؤسسي. فالاستثمار في تطوير مهارات موظفيهم وتعزيز بيئة عمل إيجابية يساهم في تحسين الأداء العام والابتكار. لذلك، يُعد فهم وتقدير قيمة العامل البشري خطوة أساسية نحو بناء مؤسسات قوية ومستدامة قادرة على مواجهة تحديات المستقبل بثقة. (الشوكة، 2020)

تُعد الهجمات الإلكترونية من أبرز التحديات التي تواجه المؤسسات والأفراد في العصر الرقمي الحديث، مع تزايد تهديدات الأمن الإلكتروني بوتيرة متسارعة. تعتمد هذه الهجمات على استغلال ثغرات الأنظمة والشبكات، مما يُعرض البيانات الحساسة للخطر، ويُلحق الضرر بسمعة الشركات وعملياتها التشغيلية. يُعدّ الفهم العميق لطبيعة هذه الهجمات وأبعادها أمراً بالغ الأهمية لحماية المعلومات والموارد الحيوية. (عوض، 2022)

تتراوح الهجمات الإلكترونية بين البرمجيات الخبيثة، وهجمات رفض الخدمة، والاحتياز الإلكتروني، ولكل منها تأثيرها الفريد على الأفراد والمؤسسات. على سبيل المثال، يُمكن للبرمجيات الخبيثة تسريب بيانات حساسة، بينما يُمكن لهجمات رفض الخدمة تعطيل الخدمات الإلكترونية والتأثير على قدرة المؤسسة على العمل بسلاسة. تزداد هذه التهديدات تعقيداً مع تطور التكنولوجيا، حيث يستخدم المهاجمون تقنيات متقدمة لتجاوز أنظمة الأمن التقليدية. (الرواشدة، 2022)

تتنوع الدوافع وراء الهجمات الإلكترونية، ويمكن أن تكون اقتصادية، أو سياسية، أو حتى شخصية. يسعى بعض المهاجمين إلى تحقيق مكاسب مالية من خلال سرقة البيانات أو ابتزاز المؤسسات، بينما قد يسعى آخرون إلى إحداث تأثير سياسي أو اجتماعي. لذا، أصبح من الضروري للمؤسسات وضع استراتيجيات شاملة لمواجهة هذه التهديدات وفهم طبيعة المخاطر التي قد تواجهها. (المقدشي، 2019)

تُعدّ التدابير الوقائية جزءاً لا يتجزأ من استراتيجية الأمن السيبراني. ويتطلب ذلك استخدام تقنيات متقدمة مثل التشفير وجدوران الحماية وأنظمة كشف التسلل، بالإضافة إلى توعية الموظفين بأهمية الأمن السيبراني. فبينما يُعدّ البشر ثروة قيمة، إلا أنهم قد يُشكلون أيضاً نقطة ضعف إذا لم يتلقوا التدريب المناسب للتعرف على التهديدات والتصدي لها. (العمرى، 2022)

تُمثّل الهجمات السيبرانية تحدياً مستمراً يتطلب تضامناً جهود جميع الجهات المعنية، بما في ذلك الحكومات والمؤسسات والأفراد. ويُعدّ التوعية بأهمية الأمن السيبراني ووضع استراتيجيات فعالة لمواجهة هذه التهديدات خطوة أساسية نحو حماية المعلومات والموارد الحيوية في عالمٍ متزايد الترابط. (الصمادي، 2023)

أهمية الدراسة

تعتمد أهمية هذه الدراسة على إسهاماتها النظرية والتطبيقية فيما يلي:

الأهمية النظرية

✓ تتناول الدراسة موضوعاً مترابطاً يجمع بين مفاهيم إدارة المخاطر والسلوك البشري والأمن السيبراني. يُعدّ هذا التكامل نادراً نسبياً في الأدبيات الأكاديمية العربية، التي غالباً ما تُركّز على الجوانب التقنية دون تناول كافٍ للبعد الإنساني للتهديدات السيبرانية.

- ✓ تُسهم الدراسة في تطوير إطار نظري جديد لفهم سلوك الأفراد داخل المؤسسات كعناصر فاعلة في منظومة التهديدات. ويتحقق ذلك من خلال تحليل العوامل المؤدية إلى الأخطاء الأمنية (مثل نقص الوعي أو الإهمال أو الجهل باللوائح الأمنية)، واقتراح آليات لإدارة هذا النوع من المخاطر ضمن منظومة أمن الشركات.
- ✓ تُساعد الدراسة على سد فجوة معرفية تتعلق بغياب التكامل الواضح بين الأدبيات التي تتناول إدارة المخاطر كوظيفة إدارية ونظريات السلوك التنظيمي التي تُفسر سلوك الأفراد في مكان العمل، لا سيما فيما يتعلق بمواجهة التهديدات السيبرانية الحديثة.
- ✓ يفتح هذا البحث المجال أمام باحثين آخرين لتطوير أدوات قياس كمية ونوعية لتقييم وعي الأفراد بالمخاطر السيبرانية والتزامهم بالإجراءات الوقائية، وربط ذلك بالنتائج الأمنية كعدد الحوادث أو معدل التفاعل مع رسائل التصيد الاحتيالي، مما يعزز الأساس العلمي في هذا المجال.
- ✓ يُثري البحث المكتبة العربية بإضافة نظرية جديدة باللغة العربية في مجال معاصر وحساس للغاية، مما يُسهم في رفع الوعي البحثي والتطبيقي للأمن السيبراني من منظور إنساني في السياق العربي.

الأهمية العملية

- ✓ تُبرز الدراسة الدور المحوري للعامل البشري كأحد أكثر نقاط الضعف شيوعاً في أنظمة الأمن السيبراني. وتُشير التقارير إلى أن نسبة كبيرة من الهجمات الناجحة تُنفذ باستغلال السلوك البشري الخاطئ، مما يجعل معالجة هذه المخاطر ضرورةً تنظيميةً وليست خياراً.
- ✓ تُقدم الدراسة خارطة طريق عملية للمؤسسات لتحديد السلوكيات البشرية المحفوفة بالمخاطر (مثل ضعف الوعي الأمني، والاستجابة المتهورة لرسائل التصيد الاحتيالي، ومشاركة كلمات المرور)، وتُقدّم تدخلات إدارية مثل التدريب والتوعية وسياسات الرقابة التي من شأنها الحد من احتمالية التعرض للاختراقات.
- ✓ تُساعد الدراسة في توجيه صانعي القرار نحو تبني سياسات أمن سيبراني أكثر شمولاً تتجاوز الأدوات التقنية، لتشمل أيضاً إدارة رأس المال البشري، ووضع برامج توعية دورية، وتقييم الأداء الفردي في التعامل مع المواقف الأمنية، مما يُعزز جاهزية المؤسسات.
- ✓ تُوفر الدراسة إطار عمل يُمكن تطبيقه في القطاعات الحساسة (مثل المالية والحكومة والتعليم والطاقة)، وهي من أكثر القطاعات استهدافاً للهجمات السيبرانية. يُساهم هذا الإطار في تعزيز أمن المعلومات على المستويين الوطني والمؤسسي.
- ✓ تُساعد الدراسة في تقليل الخسائر المالية والتشغيلية الناتجة عن نقاط الضعف البشرية، سواء المتعلقة بتعطّل النظام أو تسرب البيانات أو الإضرار بسمعة الشركات، من خلال تقديم توصيات قابلة للتطبيق في بيئات العمل الرقمية الحالية.

اهداف الدراسة

- تهدف الدراسة إلى معرفة مدى أثر تطبيق إدارة مخاطر العامل البشري بأبعادها مجمعة المتمثلة في (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد من الهجمات السيبرانية: دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية، ويتفرع منه مجموعة من الأهداف الفرعية:
- ✓ التعرف على تحديد وتقييم المخاطر ومدى انعكاسها على الحد من الهجمات السيبرانية.
- ✓ التعرف على معالجة إدارة المخاطر ومدى انعكاسها على الحد من الهجمات السيبرانية.
- ✓ التعرف على مراقبة إدارة المخاطر ومدى انعكاسها على الحد من الهجمات السيبرانية.

فروض الدراسة:

لتحقيق أهداف الدراسة والإجابة على تساؤلاتها يمكن للباحث اعتماداً على الإطار النظري المتعلق بالدراسة، واستناداً إلى نتائج الدراسات السابقة تم صياغة الفرضيات التالية:

الفرضية الرئيسية الأول: لا يوجد أثر ذو دلالة إحصائية لتطبيق إدارة مخاطر العامل البشري بأبعادها مجمعة المتمثلة في (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد من الهجمات السيبرانية: دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية

وينبثق من هذه الفرضية الفرضيات الفرعية الثلاث التالية:

- ✓ لا يوجد أثر ذو دلالة إحصائية تحديد وتقييم المخاطر ومدى انعكاسها على الحد من الهجمات السيبرانية
 - ✓ لا يوجد أثر ذو دلالة إحصائية ل معالجة إدارة المخاطر ومدى انعكاسها على الحد من الهجمات السيبرانية
 - ✓ لا يوجد أثر ذو دلالة إحصائية لمراقبة إدارة المخاطر ومدى انعكاسها على الحد من الهجمات السيبرانية
- حدود الدراسة:**

- ☑ **حدود موضوعية :** تقتصر الدراسة على تحليل أثر تطبيق إدارة مخاطر العامل البشري بأبعادها مجمعة المتمثلة في (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد من الهجمات السيبرانية
- ☑ **حدود مكانية:** تُجرى الدراسة على المؤسسات الحكومية في المملكة العربية السعودية
- ☑ **حدود زمانية :** تم إعداد الدراسة في عام 2025.
- ☑ **حدود بشرية:** تقتصر الحدود البشرية لهذه الدراسة على العاملين في المؤسسات الحكومية في المملكة العربية السعودية، ممن لديهم ارتباط مباشر بالأعمال الحكومية

الإطار النظري

المبحث الأول: فهم العوامل البشرية وتشريح الأخطاء النظامية

المقدمة

تُعَد إدارة مخاطر العامل البشري من أكثر التحديات تعقيداً في منظومة الحوكمة المؤسسية، إذ تتشابك فيها عناصر السلوك الفردي، والثقافة التنظيمية، وسياسات الموارد البشرية، والضغوط البيئية والتقنية المحيطة بالموظف. تبدأ هذه الإدارة بفهم معمق لماهية "العامل البشري" بوصفه مجموعة من القدرات والحدود النفسية والمعرفية والجسدية التي تؤثر في الأداء اليومي للأفراد. فالأخطاء الناجمة عن الإرهاق أو التوتر أو ضعف التدريب ليست حوادث معزولة، بل أعراض لنظام عمل قد يفتقر إلى التوازن بين متطلبات الإنتاج واحتياجات الإنسان. من هنا يأتي دور الإدارة في تحليل السياق الداخلي والخارجي لاكتشاف نقاط الضعف السلوكية المتكررة، مثل الاعتماد المفرط على الذاكرة، أو مقاومة التغيير، أو الثقة الزائدة في أنظمة الأتمتة، ثم تحويل هذه الاكتشافات إلى فرضيات قابلة للقياس والمتابعة . (Al-Salahi & Al-Tarawneh, 2024)

يمتد نطاق إدارة مخاطر العامل البشري إلى تصميم عمليات استقطاب وتوظيف تضع كفاءة المرشح على صعيد السلامة والسلوك الأخلاقي في مرتبة لا تقل أهمية عن الكفاءة الفنية. فالمقابلات المبنية على الكفايات، والتقييمات النفسية، واختبارات تحمل الضغط، ليست أدوات انتقائية فحسب، بل خطوط دفاع استباقية تقلص احتمال ظهور سلوكيات قد تُفضي إلى خسائر مالية أو سمعة سلبية. وبعد الاستقطاب تبرز أهمية التهيئة

الوظيفية الممنهجة التي توضّح للموظف الجديد طبيعة المخاطر المرتبطة بدوره، وتحفّزه على تبني عقلية تقدّر الإبلاغ المبكر عن المشكلات . (Al-Dhawadi, 2020)

الهندسة البشرية وتصميم بيئة العمل الآمنة

يلعب تصميم بيئة العمل دوراً محورياً في خفض احتمالية الخطأ البشري؛ فالإضاءة السيئة أو الضوضاء أو واجهات الاستخدام المعقّدة ترفع مستويات التشوّش وتزيد من زمن التفاعل مع المهام الحساسة. تعتمد المؤسسات الرائدة مبادئ الهندسة البشرية لإعادة تشكيل أماكن العمل بحيث تُوضّع الأدوات الحرجة في محيط إدراكي واضح، وتُزوّد أجهزة التحكم ببتبويضات بصرية وصوتية تمنع التشويش وتسهّل اتخاذ القرار. كما تُستخدم المحاكاة والواقع الافتراضي لتدريب الموظفين على سيناريوهات عالية الخطورة حتى يتحوّل الرد السليم إلى عادة راسخة . (Ramadan, 2022)

لا يمكن فصل إدارة مخاطر العامل البشري عن ثقافة المؤسسة في ما يتعلق بالشفافية والإفصاح. فنهج “الثقافة العادلة” يميّز بين الأخطاء غير المقصودة والسلوك المتعمّد المخالف، ويشجع الموظفين على الاعتراف بالهفوات فور وقوعها. يعتمد نجاح هذا النهج على دعم الإدارة العليا وترسيخ قيم تؤكد أن الهدف هو تحسين النظام لا البحث عن كبش فداء، لتتحول التحقيقات من محاسبة إلى أداة تعلّم تنظيمي مستمر . (Abdul Jader, 2022)

تتطلّب الرقابة الفعّالة على المخاطر البشرية بنية تقنية متقدمة تجمع بين أدوات القياس اللحظي للأداء وأدوات التحليل التنبؤي. فأنظمة مراقبة الإجهاد القابلة للارتداء تقدّم قراءات حية لمستويات الإرهاق وترتبطها بمنصات ذكاء اصطناعي تستشرف متى ترتفع احتمالية الخطأ الحرج. غير أن الاعتماد على التكنولوجيا لا يُغني عن دور القيادة؛ فالتواصل المباشر، والدعم النفسي، وبرامج التوازن بين الحياة والعمل تظل مقومات لا يمكن للأتمتة أن تعوّضها . (Awad & Al-Khazaali, 2022)

تُختتم دورة إدارة مخاطر العامل البشري بعملية مراجعة شاملة تستلهم مبادئ التحسين المستمر. تُقاس فجوات الأداء بمؤشرات كمية مثل عدد الحوادث وشدّتها، وبمقاييس نوعية كرضا الموظفين وثقتهم بالنظام. تُستخدم النتائج لتحديث سياسات التوظيف والتدريب والتقنية، فيتحوّل الجانب البشري من عامل تهديد إلى مصدر أفضلية تنافسية يرفع موثوقية العمليات ويعزّز سمعة المؤسسة . (Attia, Obaidat & Al-Saghir, 2024)

توطّر المنظمات المتقدمة إدارة مخاطر العامل البشري ضمن منظومة تشريعية ومعيارية تضمن التوافق مع القوانين المحلية والاتفاقيات الدولية. فالقطاعات عالية الحساسية تستند إلى معيار ISO 45001 ومنهجيات Crew Resource Management لضبط التعاون واتخاذ القرار تحت الضغط. تُتيح هذه الأطر لغة مشتركة لتصنيف المخاطر وتصميم ضوابط وقائية وعلاجية عابرة للحدود، وتؤسس لدورة تدقيق وتحسين تُبقي سياسات المخاطر البشرية حيّة لا موسمية . (Al-Tarawneh, Al-Jubouri & Al-Maaytah, 2020)

المبحث الثاني: الهجمات السيبرانية

المقدمة

تُعدّ واحدة من أخطر الظواهر الأمنية المعاصرة، إذ تنتقل بها الجرائم التقليدية إلى فضاء رقمي مليء بالتعقيدات التقنية والتهديدات متعددة الوجوه. يتمحور مفهوم “الهجمات السيبرانية” حول أي نشاط عدائي يستهدف الأنظمة الإلكترونية أو البنى التحتية الرقمية بهدف تعطيلها أو سرقة بياناتها أو اختراقها لتحقيق مكاسب مالية أو

سياسية أو حتى انتقامية. وتشمل هذه الهجمات مجموعة واسعة من الأساليب، من استغلال الثغرات البرمجية واستخدام برامج الفدية (Ransomware) وصولاً إلى عمليات التصيد (Phishing) التي تسعى لخداع المستخدمين وسرقة هوياتهم الرقمية. ما يجعل هذا المشهد أكثر تعقيداً هو تنامي مهارات القراصنة وصعوبة تحديد هويتهم الحقيقية، إذ يمكن إدارة الهجمة من خلال شبكات افتراضية (VPN) أو باستخدام برمجيات التخفي بحيث يصعب تتبع المصدر الفعلي . (Al-Salahi & Al-Tarawneh, 2024)

يمهد هذا المناخ لظهور هجمات منظمة تقف خلفها جهات حكومية أو مجموعات قرصنة شديدة التنظيم تُعرف باسم التهديدات المستمرة المتقدمة (Advanced Persistent Threats – APTs) تتخذ هذه المجموعات من القدرة على التخفي واستمرار التسلل ركائز أساسية، حيث تدرس الهدف بدقة وتنتظر اللحظة المناسبة لتنفيذ الهجمة أو سرقة البيانات دون إثارة الانتباه. وغالباً ما يستهدفون القطاعات الحساسة مثل الطاقة أو البنى التحتية المالية بغية إحداث اضطراب شامل، أو تجميع معلومات استخباراتية على مدى زمني طويل. (Al-Dhawadi, 2020)

يوكب ذلك تزايد مقلق في عدد الثغرات "اليوم الصفري" (Zero-Day Vulnerabilities) التي لا يتوفر لها بعد أي تحديث أمني من الشركات المطورة، مما يمنح المهاجمين فرصة ذهبية للولوج إلى شبكات الضحايا قبل أن يتمكنوا من سد هذه الفجوات . (Ramadan, 2022)

إلى جانب الهجمات المتطورة، لا يزال العنصر البشري أحد أضعف حلقات الدفاع في سلاسل الأمن السيبراني. إذ غالباً ما يتعرض الموظفون عن غير قصد لرسائل بريد خبيثة تبدو رسمية، أو ينفقون على روابط تقود إلى صفحات ومواقع مزورة، في عملية تُعرف باسم التصيد الاحتيالي. وعند تدوير كلمات مرور بسيطة أو تكرار استخدامها في أكثر من موقع، تتضاعف فرص نجاح المهاجمين في انتزاع حقوق وصول أعلى يمكنهم بواسطتها التنقل بحرية داخل البنية التحتية. ويلجأ المخترقون في أحيان كثيرة إلى تكتيكات الهندسة الاجتماعية، مستغلين فضول المستخدم أو خوفه لإقناعه بتسهيل العملية؛ فبمجرد التعرف إلى ثغرة في سلوك بشري أو ناموس تنظيمي، يستطيع القراصنة التحكم في الأنظمة وسحب ما يحتاجونه من بيانات أو حتى تدميرها.

تمتد آثار الهجمات السيبرانية أفقياً وعمودياً، فتُلحق ضرراً في جوانب قد تفوق الخسائر المالية المباشرة. ففي حال اختراق مرافق صحية مثلاً، لا يقتصر الخطر على المساس بخصوصية المرضى وسرقة بياناتهم الكبرى، بل قد يمتد ليعطل أنظمة دعم الحياة أو الأجهزة الحرجة في غرف العناية. يتشابه الأمر في قطاعات حيوية أخرى كالمطارات والمرافق الحكومية، حيث تؤدي الهجمات أحياناً إلى شلل في الخدمات الأساسية أو شيوخ حالة من الذعر العام. (Abdul Jader, 2022)

وطالما تحدثت هذه الاختراقات على نطاق واسع، تزداد معها احتمالية الإضرار بالسمعة المؤسسية وفقدان ثقة العملاء أو المستثمرين. وفي بعض الحالات قد تتعقد الأمور أكثر، عندما يتطور الأمر إلى دفع فديات مالية بمبالغ طائلة لتجنب نشر البيانات أو إعادة تشغيل الشبكات بعد تشفيرها. (Awad & Al-Khazaali, 2022)

تسعى المؤسسات الضخمة والأجهزة الحكومية على الصعيد العالمي إلى بناء حصون رقمية قادرة على صد الهجمات وتخفيف أضرارها اللاحقة؛ فتسنّ تشريعات تلزم الشركات بإبلاغ الجهات المعنية عن أي اختراق يقع، وتضع معايير للخصوصية وحماية البيانات مثل لائحة الاتحاد الأوروبي (GDPR) في المجال الأوروبي. كما تستثمر بكثافة في برمجيات مضادة للفيروسات، وجدران نارية (Firewalls)، فضلاً عن تقنيات التحليل السلوكي للأنظمة لمراقبة أي نشاط شاذ قد يشير إلى اختراق. لكن رغم هذا التحسين، تظل تلك الأساليب

الدفاعية عرضة للتحايل من جانب الخصوم الذين يملكون وصولاً إلى أدوات متطورة في سوق برمجيات الاختراق. وفي مواجهة ذلك، تتجه السياسات الأمنية الحديثة نحو تبني استراتيجية "صفر ثقة (Zero Trust)" التي تفرض مصادقات متعددة العوامل على كل طلب وصول في الشبكة، وتعامل أي نشاط لا يخضع للتحقق الكامل بوصفه نشاطاً عدائياً محتملاً، في محاولة لتجاوز الاعتماد على الجدران النارية التقليدية وحدها . (Attia, Obaidat & Al-Saghir, 2024)

دراسات سابقة

1. دراسة حلول (2019) بعنوان: إدارة المخاطر في شركات التأمين: دراسة حالة الشركة الوطنية

للتأمين SAA وكالة غليزان للفترة "2014-2016"

تهدف هذه الدراسة المتواضعة إلى تسليط الضوء على الأساليب المختلفة التي تتبعها شركات التأمين لإدارة المخاطر التي تتعرض لها خلال مزاوله أنشطتها، كما تتضمن الإفصاح والشفافية اللازمين بين هذه الشركات وجميع أصحاب المصلحة. تُعد الإدارة السليمة للمخاطر عنصراً أساسياً في قطاع التأمين في هذه المرحلة، نظراً لطبيعة هذا النشاط الذي يعتمد بشكل كبير على أساس من الثقة والشفافية لنمو الشركة واستقرارها. ولتحقيق أهداف هذه الدراسة، طرحنا مجموعة من الأسئلة على المدققين الداخليين في الهيئة، وجمعنا وحللنا مجموعة من الإجابات والمعلومات ذات الصلة بالدراسة الخاصة بالشركة. وخلصت الدراسة إلى عدة نقاط رئيسية، أهمها: - للتأمين أنواع مختلفة، تسعى جميعها إلى تقليل المخاطر التي قد تصيب الأشخاص أو الممتلكات من خلال شركات التأمين التي تدرس وتدير المخاطر المختلفة التي يتعرض لها المؤمن له. - يقوم التأمين على مبدأ تقاسم المخاطر، ويُحسب قسط التأمين بناءً على وظيفة المؤمن له أو مهنته، مما يضمن أن يكون القسط في متناوله. تُعتبر إدارة المخاطر وسيلة فعالة لمواجهة المخاطر التي تتعرض لها شركة التأمين. وأهم المخاطر التي تواجه الشركة هو خطر الإفلاس، ومجلس الإدارة هو من يضع أساليب مواجهة المخاطر التي تواجه الشركة.

2. دراسة أيوب (2019) بعنوان: دور التدقيق الداخلي في إدارة مخاطر السيولة: دراسة ميدانية

لمجموعة بنوك "بنك الفلاحة والتنمية الريفية، بنك الجزائري الخارجي، بنك الخليج الجزائري" ورقلة

تهدف هذه الدراسة إلى التعرف على التدقيق الداخلي ودوره في إدارة مخاطر السيولة في المؤسسة المالية (بنك الفلاحة والتنمية الريفية، بنك الجزائري الخارجي، بنك الخليج الجزائري)، قد استخدم المنهج الوصفي في إجراء الدراسة وقد أعد استبيان خصيصاً لهذا الغرض ومن تم توزيعها على مجتمع الدراسة البالغ عدد (30) فرداً بالبنوك السالفة الذكر في فترة امتدت من 02 ماي إلى 20 ماي 2019 م، وقد توصلت الدراسة إلى مجموعة من النتائج أهمها تمتع المدقق الداخلي بالاستقلالية الكافية لأداء مهامه، بالإضافة إلى وجود وعي لدى المدققين الداخليين بأهمية دورهم في إدارة مخاطر السيولة في البنوك وكذا تعاونهم الكبير مع الجهة المسؤولة عن تحديد المخاطر ويتمثل ذلك في تقديمهم للاستشارات والتوصيات بشأن إدارة المخاطر وكل ما يتعلق بذلك.

3. دراسة المري (2020) بعنوان: أثر إدارة المخاطر على الأداء الاستراتيجي: ذكاء الأعمال كمتغير

وسيط في البنوك التجارية العاملة في دولة الكويت

هدفت هذه الدراسة إلى التعرف على أثر إدارة المخاطر على الأداء الاستراتيجي مع استخدام ذكاء الأعمال كمتغير وسيط في البنوك التجارية العاملة في دولة الكويت. ولتحقيق أهداف الدراسة، صمم الباحث استبانة للدراسة لتوزيعها على أفراد العينة المسحوبة من مجتمع الدراسة، والتي تكونت من الموظفين العاملين في

الإدارة العليا والوسطى في البنوك التجارية العاملة في دولة الكويت، والبالغ عددهم 6462 إداريًا. وكانت العينة المسحوبة عينة عشوائية طبقية مكونة من 363 موظفًا يعملون في الإدارة العليا والوسطى في البنوك التجارية العاملة في دولة الكويت. وقد تم توزيع الاستبانة على عينة الدراسة، وتم استرداد 270 استبانة صالحة للتحليل. وقد تم التوصل إلى عدة نتائج أهمها: يوجد تأثير ذو دلالة إحصائية لإدارة المخاطر بأبعادها (مخاطر الوثائق، ومخاطر السمعة التنظيمية، ومخاطر الموارد البشرية، ومخاطر الثقافة التنظيمية) على الأداء الاستراتيجي في البنوك التجارية العاملة في دولة الكويت. هناك أيضًا تأثير لإدارة المخاطر بأبعادها (مخاطر الوثائق، ومخاطر السمعة التنظيمية، ومخاطر الموارد البشرية، ومخاطر الثقافة التنظيمية) على ذكاء الأعمال في البنوك التجارية العاملة في دولة الكويت. كما يوجد تأثير لذكاء الأعمال على الأداء الاستراتيجي في البنوك التجارية العاملة في دولة الكويت. تؤثر إدارة المخاطر على الأداء الاستراتيجي في البنوك التجارية العاملة في الكويت من خلال تفعيل ذكاء الأعمال كمتغير وسيط. ركزت أبرز التوصيات على ما يلي: ضرورة تحديث آليات إدارة المخاطر في البنوك من خلال تعيين أفراد محددين للحصول على أي بيانات للعملاء؛ الحفاظ على سمعة البنوك فيما يتعلق بإجراءات الأمن؛ تشجيع الموظفين على فصل العلاقات الشخصية عن إجراءات العمل؛ وتقليل دوران الموظفين في البنك. كما توصي الدراسة بضرورة ضمان تحديث شبكة الإنترنت في البنوك التجارية العاملة في الكويت. كما يجب على إدارة البنك التركيز على رفع مستوى الأداء الاستراتيجي من خلال التحسين المستمر للأداء المالي، بالإضافة إلى معالجة ملاحظات وشكاوى العملاء. يجب تمييز الخدمات المصرفية عن تلك التي تقدمها البنوك المنافسة، ويجب على إدارة البنك ضمان الاحتفاظ بالموظفين الأكفاء.

4. دراسة الحسني (2022) بعنوان: أثر التفكير الاستراتيجي في إدارة المخاطر: الدور المعدل للدعم

المنظمي في شركات المقاولات العمانية

هدفت الدراسة إلى قياس أثر التفكير الاستراتيجي بأبعاده (القصد الاستراتيجي، والرؤية النظامية، وصياغة الافتراضات، والتفكير في الوقت المناسب، واغتنام الفرص) على إدارة المخاطر بأبعادها (تحديد المخاطر، وتقييم المخاطر، والاستجابة للمخاطر، والسيطرة عليها) في شركات المقاولات العمانية. كما هدفت إلى توضيح الدور المعدل للدعم التنظيمي في تحسين أثر التفكير الاستراتيجي على إدارة المخاطر لهذه الشركات. تكون مجتمع الدراسة من (205) شركة تمثل شركات المقاولات العمانية. وتم الاعتماد على أسلوب المسح الشامل، حيث تم توزيع (205) استبانة، واسترجاع (149) استبانة صالحة للتحليل الإحصائي. واستخدمت الدراسة المنهج الوصفي الكمي، وتم استخدام مجموعة من الأساليب الإحصائية لتحليل بيانات الدراسة، من أهمها معامل الانحدار والانحدار الهرمي. وتوصلت الدراسة إلى عدة نتائج، من أهمها وجود أثر ذي دلالة إحصائية للتفكير الاستراتيجي على إدارة المخاطر في شركات المقاولات العمانية. أكدت الدراسة أيضًا دور الدعم التنظيمي في تعزيز أثر التفكير الاستراتيجي على إدارة المخاطر في الشركات العمانية. وكشفت عن مستويات مرتفعة لأبعاد التفكير الاستراتيجي، باستثناء صياغة الفرضيات، ومستويات مرتفعة لأبعاد إدارة المخاطر. كما جاءت أهمية الدعم التنظيمي متوسطة. وفي ضوء النتائج، اقترح الباحث مجموعة من التوصيات التي من شأنها مساعدة إدارة شركات المقاولات العمانية على رفع مستويات التفكير الاستراتيجي وإدارة المخاطر والدعم التنظيمي، وتحقيق التوازن بينهما. وأوصت بأن تعمل الشركات العمانية على تطوير قدرات المديرين على استشراف المستقبل، وتشجيعهم على إعداد السيناريوهات والافتراضات. كما أوصت باستخدام أنظمة متطورة لرصد المخاطر، والاهتمام بشكل أكبر بالاستراتيجيات البديلة لمواجهة المخاطر، وعدم الاعتماد على خطة

محددة. كما أكدت على أهمية إنشاء نظام مكافآت يتناسب مع مساهمات الموظفين، ومعاملتهم بعدالة في توزيع إجراءات العمل، وتوزيع المكافآت بشكل عادل، مما يساهم في خلق رضا والتزام الموظفين وتحسين الأداء.

5. دراسة المصري (2019) بعنوان: إدارة مخاطر الأعمال وأثرها في الميزة التنافسية: دراسة تطبيقية

في بنك صفوة الإسلامي

هدفت هذه الدراسة إلى دراسة أثر عمليات إدارة مخاطر الأعمال المالية والمصرفية (كتعبير عن مخاطر الأعمال) على الميزة التنافسية في بنك صفوة الإسلامي. ولتحقيق هدف الدراسة، تم تطوير استبانة مكونة من (فقرة واحدة) واختبار صدقها وثباتها. يتكون مجتمع الدراسة من الإدارة العليا، وإدارة الموارد البشرية، والإدارة المالية، وإدارة الفروع، وإدارة المخاطر، وإدارة التسويق، بالإضافة إلى العاملين في فروع بنك صفوة الإسلامي. بلغ حجم مجتمع الدراسة 150 مديراً بمستويات إدارية مختلفة، وتم استرداد 143 استبانة صالحة للتحليل، بنسبة استجابة بلغت 95% من المجيبين الذين يمثلون وحدة التحليل المستهدفة. وتمت المعالجة الإحصائية لاستجابات المدراء باستخدام الحزمة الإحصائية للعلوم الاجتماعية (SPSS). توصلت الدراسة إلى النتائج التالية: يوجد تأثير ذو دلالة إحصائية لعمليات إدارة المخاطر على جودة الخدمة مع دلالة ($\alpha = 0.05$) وقيمة تباين نموذج الانحدار الخطي المتعدد $F = 40.620$ وقبول فكرة نموذج الانحدار الخطي المتعدد من حيث قيمة تحليل التباين للتحقق من صحة نموذج الانحدار الخطي المتعدد، بينما بلغت القوة التفسيرية للتغير في جودة الخدمات المصرفية $R^2 = 0.541$. يوجد تأثير ذو دلالة إحصائية لعمليات إدارة المخاطر على التمايز في التعامل مع العملاء، مع دلالة ($\alpha < 0.05$)، وقيمة تباين نموذج الانحدار الخطي المتعدد $F = 25.671$ وقبول فكرة نموذج الانحدار الخطي المتعدد، من حيث قيمة تحليل التباين للتحقق من صحة نموذج الانحدار الخطي المتعدد، بينما بلغت القوة التفسيرية للتغير في جودة الخدمات المصرفية $R^2 = 0.427$. يوجد تأثير ذو دلالة إحصائية لعمليات إدارة المخاطر على الابتكار في برامج تقديم الخدمات للعملاء، مع دلالة ($\alpha = 0.05$)، وقيمة تباين نموذج الانحدار الخطي المتعدد $F = 29.225$ ، ويتم قبول فكرة نموذج الانحدار الخطي المتعدد، من حيث قيمة تحليل التباين للتحقق من صحة نموذج الانحدار الخطي المتعدد، بينما بلغت القوة التفسيرية للتغير في جودة الخدمات المصرفية $R^2 = 0.459$. يوجد تأثير ذو دلالة إحصائية لعمليات إدارة المخاطر على توقيت تقديم الخدمات، مع دلالة ($\alpha = 0.05$)، وقيمة تباين نموذج الانحدار الخطي المتعدد $F = 32.025$ ، والقوة التفسيرية للتغير في جودة الخدمات المصرفية $R^2 = 0.459$. تم قبول نموذج الانحدار الخطي المتعدد بالاعتماد على تحليل التباين (ANOVA) للتحقق من صحة نموذج الانحدار الخطي المتعدد، بينما بلغت القوة التفسيرية للتغير في جودة الخدمات المصرفية $R^2 = 0.481$. واقتُرحت الدراسة ضرورة تعميق الوعي المعرفي بعمليات إدارة المخاطر من خلال إعطاء الأولوية لعمليات تقييم المخاطر، ثم خيارات التعامل معها. كما اقتُرحت الدراسة تعزيز الميزة التنافسية من حيث الحفاظ على توقيت تقديم الخدمة، والاهتمام بأنواع الابتكار في تقديم الخدمات للعملاء (المالية، والمصرفية، والإلكترونية، والخدمية) بهدف بناء جسور التواصل معهم بأساليب ذكية وفعالة.

6. دراسة ملوك (2019) بعنوان: دور شركات التأمين في إدارة المخاطر الصناعية: دراسة ميدانية

للشركة الجزائرية للتأمين وإعادة التأمين "La CAAR" وكالة غليزان - رقم 414

تهدف هذه الدراسة إلى إبراز دور وأهمية شركات التأمين وإعادة التأمين في إدارة جميع المخاطر، وخاصة المخاطر الصناعية. ويتحقق ذلك من خلال تطوير أنظمة لإدارتها وأساليب التعامل معها ومواجهتها من

خلال التأمين أو تحويلها إلى إعادة التأمين. وقد تحقق ذلك من خلال تناول وسائل إدارة المخاطر المختلفة، باعتبارها الوظيفة التي تضمن بقاء واستمرارية شركات التأمين والمؤسسات الأخرى في ظل الظروف البيئية المتغيرة والمعقدة. ولتوضيح ذلك، اعتمدنا على استبيان، حيث وزعنا 60 استمارة على موظفي وكالة LA CAAR للتأمين وإعادة التأمين. وبعد جمع الاستثمارات الصالحة للدراسة، قمنا بتحليلها باستخدام برنامج التحليل الإحصائي SPSS 20. وخلصنا إلى أن وكالات التأمين وإعادة التأمين تلعب دورًا أساسيًا في إدارة المخاطر الصناعية من خلال توفير أساليب وأنظمة لمواجهةها، بهدف ضمان البقاء والاستمرارية.

7. دراسة محمد (2020) بعنوان: إطار عمل لإدارة مخاطر مياه السدود: دراسة حالة النيل الشرقي

تهدف الدراسة إلى بناء إطار عمل لإدارة المخاطر المحتملة ووضع استراتيجيات واضحة للتعامل معها. ويتحقق ذلك من خلال تطوير نظام إلكتروني يساهم في إدخال البيانات وعرضها واستخراج التفاصيل والبيانات التاريخية لمساعدة متخذي القرار من جميع القطاعات (الحكومة والكهرباء والبيئة والمجتمع والجيولوجيا) على اتخاذ قرارات سليمة بناءً على بيانات واضحة ودقيقة. وقد تم استخدام المنهج الوصفي العلمي لبناء الإطار من خلال تحليل مكوناته باستخدام لغة النمذجة الموحدة (UML) واستخدام لغات تصميم الويب (PHP-HTML-CSS) لبناء النظام وتنفيذه. ومن أهم نتائج الدراسة أن النظام الجديد ساعد في استخراج معلومات دقيقة تساعد في عملية اتخاذ القرار. وقدمت توصيات لاستكمال الإطار وتحسينه ودمجه مع عدد من الوزارات. ولعله في الحكومة الإلكترونية يكون لبنة لبناء أفكار أسمى تساعد السودان على التقدم والتطور.

8. دراسة ونزار (2019) بعنوان: إدارة المخاطر في البنوك التجارية وفق ESG: حالة عينة من

البنوك التجارية العاملة في الجزائر - حاسي مسعود

هدفت هذه الدراسة إلى دراسة العلاقة بين تبني معايير الحوكمة البيئية والاجتماعية والمؤسسية (ESG) في منح الائتمان وإدارة المخاطر في البنوك. وقد استندت الدراسة إلى استبيان تم توزيعه على الموظفين الرئيسيين في البنوك التجارية العاملة في حاسي مسعود بولاية ورقلة خلال الفترة 2018-2019. وخلصت الدراسة إلى وجود اتجاه نحو تبني معايير الحوكمة البيئية والاجتماعية والمؤسسية في الإدارة ومنح الائتمان من خلال بُعد معايير الحوكمة. وخلصت الدراسة إلى أن البنوك في عينة الدراسة تركز على إدارة المخاطر من خلال المؤشرات الكمية والتقليدية، في حين أن المؤشرات غير الكمية لا تزال في مراحلها الأولى من التطوير. كما خالصنا إلى وجود علاقة ذات دلالة إحصائية بين نموذج معايير الحوكمة البيئية والاجتماعية والمؤسسية وإدارة المخاطر من خلال تأثير بُعد المعايير الاجتماعية على المتغير التابع "إدارة المخاطر" في البنوك قيد الدراسة. كما أشارت نتائج تحليل التباين أحادي الاتجاه إلى عدم وجود فروق ذات دلالة إحصائية في تطبيق إدارة المخاطر، في حين توجد فروق في تبني نموذج معايير الحوكمة البيئية والاجتماعية والمؤسسية بين البنوك التجارية قيد الدراسة.

9. دراسة أيوب (2019) بعنوان: دور التدقيق الداخلي في إدارة مخاطر السيولة: دراسة ميدانية

لمجموعة بنوك "بنك الفلاحة والتنمية الريفية، بنك الجزائري الخارجي، بنك الخليج الجزائري" ورقلة

تهدف هذه الدراسة إلى التعرف على التدقيق الداخلي ودوره في إدارة مخاطر السيولة في المؤسسات المالية (بنك الزراعة والتنمية الريفية، البنك الجزائري الخارجي، بنك الجزائر والخليج). وقد استخدم المنهج الوصفي في إجراء الدراسة، حيث تم إعداد استبيان خصيصًا لهذا الغرض ثم توزيعه على مجتمع الدراسة البالغ (30) فردًا في البنوك المذكورة خلال الفترة الممتدة من 2 مايو إلى 20 مايو 2019. وقد توصلت الدراسة إلى مجموعة من النتائج أهمها أن المدقق الداخلي يتمتع باستقلالية كافية لأداء مهامه، بالإضافة إلى وجود وعي

لدى المدققين الداخليين بأهمية دورهم في إدارة مخاطر السيولة في البنوك، وكذلك تعاونهم الكبير مع الجهة المسؤولة عن تحديد المخاطر، والذي يتمثل في تقديمهم الاستشارات والتوصيات فيما يتعلق بإدارة المخاطر وكل ما يتعلق بها.

10. دراسة جلول (2019) بعنوان: إدارة المخاطر في شركات التأمين: دراسة حالة الشركة

الوطنية للتأمين SAA وكالة غليزان للفترة "2014-2016"

تهدف هذه الدراسة المتواضعة إلى تسليط الضوء على الأساليب المختلفة التي تتبعها شركات التأمين لإدارة المخاطر التي تتعرض لها خلال مزاولة أنشطتها، كما تتضمن الإفصاح والشفافية اللازمين بين هذه الشركات وجميع أصحاب المصلحة. تُعد الإدارة السليمة للمخاطر عنصراً أساسياً في قطاع التأمين في هذه المرحلة، نظراً لطبيعة هذا النشاط الذي يعتمد بشكل كبير على أساس من الثقة والشفافية لنمو الشركة واستقرارها. ولتحقيق أهداف هذه الدراسة، طرحنا مجموعة من الأسئلة على المدققين الداخليين في الهيئة، وجمعنا وحللنا مجموعة من الإجابات والمعلومات ذات الصلة بالدراسة الخاصة بالشركة. وخلصت الدراسة إلى عدة نقاط رئيسية، أهمها: - للتأمين أنواع مختلفة، تسعى جميعها إلى تقليل المخاطر التي قد تصيب الأشخاص أو الممتلكات من خلال شركات التأمين التي تدرس وتدير المخاطر المختلفة التي يتعرض لها المؤمن له. - يقوم التأمين على مبدأ تقاسم المخاطر، ويُحسب قسط التأمين بناءً على وظيفة المؤمن له أو مهنته، مما يضمن أن يكون القسط في متناوله. تُعتبر إدارة المخاطر وسيلة فعالة لمواجهة المخاطر التي تتعرض لها شركة التأمين. وأهم المخاطر التي تواجه الشركة هو خطر الإفلاس، ومجلس الإدارة هو من يضع أساليب مواجهة المخاطر التي تواجه الشركة.

منهجية وإجراءات الدراسة

مقدمة

يتناول هذا الفصل الدراسة الميدانية وذلك من خلال التعرف على منهجية الدراسة ومجتمع وعينة الدراسة وأداة الدراسة ومصادر جمع البيانات والأساليب الإحصائية المستخدمة في الدراسة وحساب الصدق والثبات لأداة الدراسة

منهجية البحث:

يستند البحث على منهجاً وصفيّاً تحليلياً، حيث يركز على فحص الأسس النظرية المتعلقة بالموضوع من خلال استعراض المراجع العربية والأجنبية ذات الصلة. ويتضمن البحث أيضاً تنفيذ دراسة ميدانية تتمثل في توزيع استبيانات على فئات مختلفة من العينة المختارة.

مجتمع وعينة الدراسة

تمثل مجتمع الدراسة في العاملين في قسم إدارة الأزمات بوزارة الصحة دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية وقامت الدراسة باستخدام أسلوب العينات العشوائية البسيطة لجمع بيانات الدراسة وذلك عن طريق أداة الدراسة المتمثلة في استمارة الاستبيان وقد بلغ عدد أفراد عينة الدراسة 350 فرد وهم الذين أجابوا على اسئلة استمارة الاستبيان.

مصادر جمع البيانات والمعلومات:

تعتمد الدراسة على مصدرين أساسيين في جمع البيانات والمعلومات كما يلي:

- **المصادر الثانوية:** وتتمثل في الكتب والمراجع العربية والأجنبية ذات الصلة بموضوع الدراسة بالإضافة إلى الاعتماد على الأبحاث والدراسات السابقة والدوريات والمجلات العلمية والمقالات
- **المصادر الأولية:** حيث تعتمد الدراسة على الاستبانة كأداة رئيسية في جمع البيانات من مصادرها والتي تم تصميمها خصيصاً لهذا الغرض على Google Forms وإرسال رابطها إلى مجتمع الدراسة

الأساليب الإحصائية:

قام البحث باستخدام البرنامج الإحصائي SPSS لتحليل بيانات الدراسة باستخدام مجموعة من الأساليب الإحصائية كما يلي:

- **معامل الفاكورنباخ** لحساب مستوي ثبات أداة الدراسة
- **معامل ارتباط بيرسون** لتحديد مستوي الاتساق الداخلي وصدق أداة الدراسة وللتعرف على العلاقة بين متغيرات الدراسة
- **النسب والتكرارات** لوصف خصائص عينة الدراسة
- **الوسط الحسابي والانحراف المعياري** لوصف مستوي استجابة افراد عينة الدراسة لعبارات أداة الدراسة
- **معادلة الانحدار الخطي البسيط** لقياس الأثر بين متغيرات الدراسة

أداة الدراسة

تم العمل على الاستبانة للتناسب مع متغيرات الدراسة من خلال الاطلاع على الدراسات السابقة المتعلقة بموضوع الدراسة، حيث تكونت من قسمين رئيسيين هما:

- **القسم الأول:** وهو الجزء الخاص بالمتغيرات الديمغرافية لأفراد عينة الدراسة، والمتمثلة بـ: النوع الاجتماعي، والعمر، والمؤهل العلمي، والوضع المهني،
- **القسم الثاني:** اشتمل القسم الثاني على الفقرات والأبعاد التي تقيس متغيرات الدراسة المستقل والتابع. وتضمنت العبارات المتعلقة بالمتغير المستقل (إدارة مخاطر العامل البشري) وتضمن ثلاث ابعاد (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) واشتملت على 15 عبارات والعبارات المتعلقة بالمتغير التابع (الحد من الهجمات السيبرانية) دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية واشتملت على 10 عبارة وتم استخدام مقياس ليكرت ذو الخمس درجات الذي يتكون من موافق جداً (5)، موافق (4)، محايد (3)، غير موافق (2)، غير موافق جداً (1) في الإجابة على أسئلة محاور الدراسة.

وقد قامت الدراسة بتقسيم اتجاه موافقة أفراد عينة الدراسة على عبارات محاور الدراسة إلى مستويات من خلال تطبيق ما يلي:

- مدي المقياس = أعلى رقم في المقياس (5) - أقل رقم في المقياس (1) = 4
- مدي المستوي = مدي المقياس / عدد المستويات (5) = 0.80

جدول (1) مستويات موافقة عينة الدراسة على عبارات أداة الدراسة

الدرجة	المستوي
1 - 1.79	منخفضة جداً
1.80 - 2.59	منخفضة
2.60 - 3.39	متوسطة
3.40 - 4.19	مرتفعة

صدق أداة الدراسة

تم حساب صدق عبارات استمارة الاستبيان عن طريق تحديد مستوي التجانس الداخلي من خلال التعرف على الدلالة الإحصائية لمعاملات الارتباط بيرسون بين درجة العبارة والدرجة الكلية للمحور الذي تنتمي إليه العبارة وجاءت النتائج كما يلي:

☒ المحور الأول: إدارة مخاطر العامل البشري

جدول (2) معاملات الارتباط لعبارات المحور الأول

م	العبارة	معامل ارتباط بيرسون	Sig
تحديد وتقييم المخاطر			
1	تقوم المؤسسة بتحديد المخاطر البشرية المحتملة التي قد تؤثر على أمن المعلومات.	0.588**	0.000
2	يتم تقييم تأثير العامل البشري ضمن تحليل شامل لمصادر التهديد السيبراني.	0.687**	0.000
3	تستخدم أدوات تقييم مهنية لرصد السلوكيات البشرية التي قد تؤدي إلى اختراقات أمنية.	0.481**	0.000
4	تعتمد المؤسسة على بيانات سابقة لتحليل الحوادث المرتبطة بالعامل البشري.	0.607**	0.000
5	يتم تضمين الموظفين في عمليات تحديد المخاطر المتعلقة بالأمن السيبراني.	0.646**	0.000
معالجة إدارة المخاطر			
6	توفر المؤسسة برامج تدريبية متخصصة للتقليل من أخطاء العامل البشري.	0.778**	0.000
7	توجد سياسات واضحة للتعامل مع السلوكيات التي تهدد أمن المعلومات.	0.590**	0.000
8	يتم تطوير خطط عمل لمعالجة الثغرات التي يسببها العامل البشري.	0.782**	0.000
9	تعتمد المؤسسة حلاً تقنيًا تقلل من احتمالية حدوث الخطأ البشري.	0.795**	0.000
10	تشارك إدارة الموارد البشرية في خطط تقليل المخاطر السيبرانية الناتجة عن الموظفين.	0.488**	0.000
مراقبة إدارة المخاطر			
11	تراقب المؤسسة بشكل دوري سلوك الموظفين المتعلق باستخدام الأنظمة الإلكترونية.	0.721**	0.000
12	توجد آليات إنذار مبكر لاكتشاف أي نشاط غير معتاد ناتج عن العنصر البشري.	0.730**	0.000
13	يتم تحديث إجراءات المراقبة بشكل دوري لمواكبة تطور التهديدات البشرية.	0.529**	0.000
14	يتم توثيق ومراجعة حوادث الاختراق الناتجة عن العامل البشري بشكل منتظم.	0.634**	0.000
15	يتم إعداد تقارير دورية حول التزام الموظفين بسياسات الأمن السيبراني.	0.671**	0.000

** ذات دلالة إحصائية عند 0.01

وتبين أن جميع معاملات الارتباط لجميع عبارات محور إدارة مخاطر العامل البشري كانت ذات دلالة إحصائية عند مستوى معنوية (0.01) وهذا يعني أن عبارات محور إدارة مخاطر العامل البشري تتمتع بصدق الاتساق الداخلي وهي صالحة لأغراض الدراسة.

☒ المحور الثاني: الحد من الهجمات السيبرانية

جدول (3) معاملات الارتباط لعبارات المحور الثاني

م	العبارة	معامل ارتباط بيرسون	Sig
1	تمتلك المؤسسة خطة استجابة واضحة للهجمات السيبرانية.	0.694**	0.000
2	تُحدَّث أنظمة الحماية بشكل مستمر لتقليل احتمالية الهجمات.	0.709**	0.000
3	تعتمد المؤسسة على أدوات متقدمة لرصد التهديدات السيبرانية.	0.649**	0.000
4	يتم اختبار أنظمة الأمن السيبراني بانتظام للتأكد من كفاءتها.	0.725**	0.000
5	يتم التعامل مع أي محاولة اختراق بسرعة وفعالية.	0.652**	0.000
6	توجد آليات تحقق متعددة الهوية (MFA) لحماية الأنظمة.	0.750**	0.000
7	تُجرى محاكاة دورية لهجمات سيبرانية للتدريب على مواجهتها.	0.448**	0.000
8	تُستخدم حلول تشفير قوية لحماية البيانات الحساسة.	0.649**	0.000
9	يتم تقييم المخاطر السيبرانية الجديدة عند كل تحديث للنظام.	0.630**	0.000
10	تعتمد المؤسسة إجراءات صارمة للحد من وصول غير المصرح به إلى المعلومات.	0.673**	0.000

** ذات دلالة احصائية عند 0.01

وتبين أن جميع معاملات الارتباط لجميع عبارات محور الحد من الهجمات السيبرانية كانت ذات دلالة إحصائية عند مستوى معنوية (0.01) وهذا يعني أن عبارات محور الحد من الهجمات السيبرانية تتمتع بصدق الاتساق الداخلي وهي صالحة لأغراض الدراسة.

ثبات أداة الدراسة:

تم حساب معامل ألفا كرونباخ لعبارات محاور الاستبيان وكانت النتائج كما يلي:

جدول (4) معامل الثبات لمحاور استمارة الاستبيان

المحاور	معامل الفا كرونباخ	عدد العبارات
إدارة مخاطر العامل البشري	0.850	20
الحد من الهجمات السيبرانية	0.898	10
إجمالي استمارة الاستبيان	0.929	30

يتبين أن قيمة معامل الثبات Alpha أكبر من 0.7 لجميع محاور استمارة الاستبيان مما يؤكد على صلاحية وارتباط عبارات محاور استمارة الاستبيان وارتفاع مستوى ثبات أداة الدراسة مما يسمح باستخدام الأداة لغرض الدراسة.

تحليل النتائج

مقدمة

سوف نتناول في هذا الفصل تحليل بيانات الدراسة من خلال تحليل استمارة الاستبيان والتعرف على خصائص عينة الدراسة وتحليل محاور الدراسة واختبار فروض الدراسة من أجل تحقيق أهداف الدراسة والوصول إلى نتائج وتوصيات للدراسة.

خصائص عينة الدراسة

جدول (5) توزيع عينة الدراسة وفقاً لخصائصها

الخاصية	الفئات	العدد	%
النوع الاجتماعي	ذكر	250	71.4
	أنثى	100	28.5

الخاصية	الفئات	العدد	%
العمر	أقل من 25 سنة	60	17.1
	من 25 الى أقل من 35 سنة	100	28.5
	من 35 الى أقل من 45 سنة	100	28.5
	45 سنة فأكثر	90	25.7
المؤهل العلمي	ثانوي	90	25.7
	بكالوريوس	130	37.1
	ماجستير	100	28.5
	دكتوراه	30	8.5
الوضع المهني	مدير	150	42.8
	نائب مدير	120	34.2
	رئيس قسم	80	22.8

تحليل استمارة الاستبيان

✓ المحور الأول: إدارة مخاطر العامل البشري

1- تحديد وتقييم المخاطر

جدول (6) المتوسط الحسابي والانحراف المعياري والترتيب ومستوى الموافقة على عبارات تحديد وتقييم المخاطر

العبرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	مستوى الموافقة
تقوم المؤسسة بتحديد المخاطر البشرية المحتملة التي قد تؤثر على أمن المعلومات.	4.253	0.683	4	مرتفع جدا
يتم تقييم تأثير العامل البشري ضمن تحليل شامل لمصادر التهديد السيبراني.	4.276	0.766	2	مرتفع جدا
تستخدم أدوات تقييم مهنية لرصد السلوكيات البشرية التي قد تؤدي إلى اختراقات أمنية.	4.198	0.773	5	مرتفع
تعتمد المؤسسة على بيانات سابقة لتحليل الحوادث المرتبطة بالعامل البشري.	4.372	0.564	1	مرتفع جدا
يتم تضمين الموظفين في عمليات تحديد المخاطر المتعلقة بالأمن السيبراني.	4.273	0.775	3	مرتفع جدا
المتوسط	4.274	0.712		مرتفع

تم ترتيب عبارات تحديد وتقييم المخاطر من حيث درجة الأهمية النسبية (قيمة المتوسط الحسابي الأكبر) من وجهة نظر عينة الدراسة تبين أن عبارة (تعتمد المؤسسة على بيانات سابقة لتحليل الحوادث المرتبطة بالعامل البشري) هي أكثر العبارات أهمية بقيمة 4.372 وانحراف معياري 0.564 وبدرجة موافقة مرتفعة جدا بينما كانت العبارة (تستخدم أدوات تقييم مهنية لرصد السلوكيات البشرية التي قد تؤدي إلى اختراقات أمنية) هي أقل العبارات أهمية بقيمة 4.198 وانحراف معياري 0.773 وبدرجة موافقة مرتفعة وعند دراسة عبارات تحديد وتقييم المخاطر تبين أن اربع عبارات في مستوى الموافقة المرتفع جدا وعبارة واحدة في مستوى الموافقة المرتفع

مما يوضح وجود مستوي مرتفع جداً من تحديد وتقييم المخاطر كأحد ابعاد إدارة مخاطر العامل البشري حيث بلغت قيمة المتوسط الحسابي 4.274 بانحراف معياري 0.712

2- معالجة إدارة المخاطر

جدول (7) المتوسط الحسابي والانحراف المعياري والترتيب ومستوي الموافقة على عبارات معالجة إدارة

المخاطر

العبارة	المتوسط الحسابي	الانحراف المعياري	الترتيب	مستوي الموافقة
توفر المؤسسة برامج تدريبية متخصصة للتقليل من أخطاء العامل البشري.	4.359	0.709	2	مرتفع جداً
توجد سياسات واضحة للتعامل مع السلوكيات التي تهدد أمن المعلومات.	4.161	0.758	5	مرتفع
يتم تطوير خطط عمل لمعالجة الثغرات التي يسببها العامل البشري.	4.253	0.659	4	مرتفع جداً
تعتمد المؤسسة حلاً تقنيّة تقلل من احتمالية حدوث الخطأ البشري.	4.396	0.634	1	مرتفع جداً
تشارك إدارة الموارد البشرية في خطط تقليل المخاطر السيبرانية الناتجة عن الموظفين.	4.315	0.615	3	مرتفع جداً
المتوسط	4.297	0.675		مرتفع جداً

تم ترتيب عبارات معالجة إدارة المخاطر من حيث درجة الأهمية النسبية (قيمة المتوسط الحسابي الأكبر) من وجهة نظر عينة الدراسة تبين أن عبارة (تعتمد المؤسسة حلاً تقنيّة تقلل من احتمالية حدوث الخطأ البشري) هي أكثر العبارات أهمية بقيمة 4.396 وانحراف معياري 0.634 وبدرجة موافقة مرتفعة جداً بينما كانت العبارة (توجد سياسات واضحة للتعامل مع السلوكيات التي تهدد أمن المعلومات) هي أقل العبارات أهمية بقيمة 4.161 وانحراف معياري 0.758 وبدرجة موافقة مرتفعة وعند دراسة عبارات معالجة إدارة المخاطر تبين أن أربع عبارات في مستوى الموافقة المرتفع جداً وعبارة واحدة في مستوى الموافقة المرتفع مما يوضح وجود مستوي مرتفع جداً من معالجة إدارة المخاطر كأحد ابعاد إدارة مخاطر العامل البشري حيث بلغت قيمة المتوسط الحسابي 4.297 بانحراف معياري 0.675

3- مراقبة إدارة المخاطر

جدول (8) المتوسط الحسابي والانحراف المعياري والترتيب ومستوي الموافقة على عبارات مراقبة إدارة

المخاطر

العبارة	المتوسط الحسابي	الانحراف المعياري	الترتيب	مستوي الموافقة
تراقب المؤسسة بشكل دوري سلوك الموظفين المتعلق باستخدام الأنظمة الإلكترونية.	4.375	0.564	3	مرتفع جداً
توجد آليات إنذار مبكر لاكتشاف أي نشاط غير معتاد ناتج عن العنصر البشري.	4.453	0.539	1	مرتفع جداً
يتم تحديث إجراءات المراقبة بشكل دوري لمواكبة تطور التهديدات البشرية.	4.391	0.633	2	مرتفع جداً

مرتفع جدا	4	0.731	4.266	يتم توثيق ومراجعة حوادث الاختراق الناتجة عن العامل البشري بشكل منتظم.
مرتفع جدا	5	0.773	4.216	يتم إعداد تقارير دورية حول التزام الموظفين بسياسات الأمن السيبراني.
مرتفع جدا		0.648	4.340	المتوسط

تم ترتيب عبارات مراقبة إدارة المخاطر من حيث درجة الأهمية النسبية (قيمة المتوسط الحسابي الأكبر) من وجهة نظر عينة الدراسة تبين أن عبارة (توجد آليات إنذار مبكر لاكتشاف أي نشاط غير معتاد ناتج عن العنصر البشري) هي أكثر العبارات أهمية بقيمة 4.453 وانحراف معياري 0.539 وبدرجة موافقة مرتفعة جدا بينما كانت العبارة (يتم إعداد تقارير دورية حول التزام الموظفين بسياسات الأمن السيبراني) هي أقل العبارات أهمية بقيمة 4.216 وانحراف معياري 0.773 وبدرجة موافقة مرتفعة وعند دراسة عبارات مراقبة إدارة المخاطر تبين أن جميع العبارات في مستوى الموافقة المرتفع جدا مما يوضح وجود مستوى مرتفع جدا من مراقبة إدارة المخاطر كأحد ابعاد إدارة مخاطر العامل البشري حيث بلغت قيمة المتوسط الحسابي 4.340 بانحراف معياري 0.648

✓ المحور الثاني: الحد من الهجمات السيبرانية

جدول (9) المتوسط الحسابي والانحراف المعياري والترتيب ومستوي الموافقة على عبارات الحد من الهجمات السيبرانية

العبرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	مستوي الموافقة
تمتلك المؤسسة خطة استجابة واضحة للهجمات السيبرانية.	4.169	0.953	3	مرتفع
تُحدَّث أنظمة الحماية بشكل مستمر لتقليل احتمالية الهجمات.	4.076	0.796	7	مرتفع
تعتمد المؤسسة على أدوات متقدمة لرصد التهديدات السيبرانية.	4.091	0.855	5	مرتفع
يتم اختبار أنظمة الأمن السيبراني بانتظام للتأكد من كفاءتها.	4.154	0.678	4	مرتفع
يتم التعامل مع أي محاولة اختراق بسرعة وفعالية.	4.010	0.754	8	مرتفع
توجد آليات تحقق متعددة الهوية (MFA) لحماية الأنظمة.	3.982	0.780	9	مرتفع
تُجرى محاكاة دورية لهجمات سيبرانية للتدريب على مواجهتها.	4.078	0.764	6	مرتفع
تُستخدم حلول تشفير قوية لحماية البيانات الحساسة.	3.917	0.907	10	مرتفع
يتم تقييم المخاطر السيبرانية الجديدة عند كل تحديث للنظام.	4.221	0.667	2	مرتفع جدا
تعتمد المؤسسة إجراءات صارمة للحد من وصول غير المصرح به إلى المعلومات.	4.250	0.596	1	مرتفع جدا
المتوسط	4.095	0.775		مرتفع

تم ترتيب عبارات الحد من الهجمات السيبرانية من حيث درجة الأهمية النسبية (قيمة المتوسط الحسابي الأكبر) من وجهة نظر عينة الدراسة تبين أن عبارة (تعتمد المؤسسة إجراءات صارمة للحد من وصول غير المصرح به إلى المعلومات) هي أكثر العبارات أهمية بقيمة 4.250 وانحراف معياري 0.596 وبدرجة موافقة مرتفعة جدا بينما كانت العبارة (تستخدم حلول تشفير قوية لحماية البيانات الحساسة) هي أقل العبارات أهمية بقيمة 3.917 وانحراف معياري 0.907 وبدرجة موافقة مرتفعة وعند دراسة عبارات الحد من الهجمات السيبرانية تبين أن عبارتين في مستوى الموافقة المرتفع جدا وثمانية عبارات في مستوى الموافقة المرتفع مما يوضح ارتفاع مستوى الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية المحدودة حيث بلغت قيمة المتوسط الحسابي 4.095 بانحراف معياري 0.775.

اختبار فروض الدراسة

❖ **الفرضية الرئيسية:** لا يوجد أثر ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) لإدارة مخاطر العامل البشري بأبعادها (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية

جدول (10) نتائج نموذج الانحدار الخطي البسيط لأثر إدارة مخاطر العامل البشري على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية

P-VALUE	R	R ²	F	T	B
0.000	0.769	0.592	**553.350	**23.523	0.992

المصدر: نتائج التحليل الإحصائي ببرنامج SPSS 23

** ذات دلالة إحصائية عند 0.01

يتبين من الجدول (10) وجود أثر طردي ذي دلالة إحصائية لمستوى إدارة مخاطر العامل البشري بأبعادها (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى 0.05 حيث كانت قيمة ($\text{Sig F} = 0.000$) وهي قيمة أقل من 0.05 أي أن قيمة F المحسوبة أكبر من قيمة F الجدولية واتضح وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية بين إدارة مخاطر العامل البشري بأبعادها (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى معنوية 0.05 واتضح أن المتغير المستقل (إدارة مخاطر العامل البشري) يفسر 76.9 % من التغيرات التي تحدث في المتغير التابع (الحد من الهجمات السيبرانية) وإن باقي التغيرات ترجع لمتغيرات أخرى لم تدخل في النموذج وتبين أن كلما ازداد مستوى إدارة مخاطر العامل البشري بمقدار 1 % ازداد مستوى إدارة مخاطر العامل البشري بأبعادها (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية بمقدار 0.446% مما يبين عدم صحة الفرضية الرئيسية للدراسة.

❖ **الفرضية الفرعية الأولى:** لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \geq 0.005$) لتحديد وتقييم المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية ، مع الدور الوسيط للالتزام المنظمة بتطبيق معايير السلامة.

جدول (11) نتائج نموذج الانحدار الخطي البسيط لأثر تحديد وتقييم المخاطر على الحد من الهجمات

السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية

P-VALUE	R	R ²	F	T	B
0.000	0.746	0.557	**480.129	**21.912	0.361

المصدر: نتائج التحليل الإحصائي ببرنامج SPSS 23

** ذات دلالة إحصائية عند 0.01

يتبين من الجدول (11) وجود أثر طردي ذي دلالة إحصائية لمستوى تحديد وتقييم المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى 0.05 حيث كانت قيمة (Sig F) = 0.000 وهي قيمة أقل من 0.05 أي أن قيمة F المحسوبة أكبر من قيمة F الجدولية واتضح وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية بين تحديد وتقييم المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى معنوية 0.05 واتضح أن المتغير المستقل (تحديد وتقييم المخاطر) يفسر 55.7 % من التغيرات التي تحدث في المتغير التابع (الحد من الهجمات السيبرانية) وأن باقي التغيرات ترجع لمتغيرات أخرى لم تدخل في النموذج وتبين أن كلما ازداد مستوى تحديد وتقييم المخاطر بمقدار 1 % ازداد مستوى للتخطيط الاستراتيجي على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية بمقدار 0.361% مما يبين عدم صحة الفرضية الفرعية الأولى للدراسة.

❖ **الفرضية الفرعية الثانية:** لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \geq 0.005$)

لمعالجة إدارة المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية من خلال الدور الوسيط لتوفير المعدات والوسائل الوقائية.

جدول (12) نتائج نموذج الانحدار الخطي البسيط لأثر معالجة إدارة المخاطر على الحد من الهجمات

السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية

P-VALUE	R	R ²	F	T	B
0.000	0.694	0.481	**354.427	**18.826	0.337

المصدر: نتائج التحليل الإحصائي ببرنامج SPSS 23

** ذات دلالة إحصائية عند 0.01

يتبين من الجدول (12) وجود أثر طردي ذي دلالة إحصائية لمستوى معالجة إدارة المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى 0.05 حيث كانت قيمة (Sig F) = 0.000 وهي قيمة أقل من 0.05 أي أن قيمة F المحسوبة أكبر من قيمة F الجدولية واتضح وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية بين معالجة إدارة المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى معنوية 0.05 واتضح أن المتغير المستقل (معالجة إدارة المخاطر) يفسر 48.1 % من التغيرات التي تحدث في المتغير التابع (الحد من الهجمات السيبرانية) وأن باقي التغيرات ترجع لمتغيرات أخرى لم تدخل في النموذج وتبين أن كلما ازداد مستوى معالجة إدارة المخاطر بمقدار 1 % ازدادت الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية بمقدار 0.337 % مما يبين عدم صحة الفرضية الفرعية الثانية للدراسة.

❖ **الفرضية الفرعية الثالثة:** لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \geq 0.005$) لمراقبة

إدارة المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية، مع اختبار الدور الوسيط للإبلاغ والاستجابة للحوادث المهنية

جدول (13) نتائج نموذج الانحدار الخطي البسيط لأثر مراقبة إدارة المخاطر على الحد من الهجمات

السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية

P-VALUE	R	R ²	F	T	B
0.000	0.650	0.422	**279.317	**16.713	0.294

المصدر: نتائج التحليل الإحصائي ببرنامج SPSS 23

** ذات دلالة إحصائية عند 0.01

يتبين من الجدول (13) وجود أثر طردي ذي دلالة إحصائية لمستوى مراقبة إدارة المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى 0.05 حيث كانت قيمة (Sig F) = 0.000 وهي قيمة أقل من 0.05 أي أن قيمة F المحسوبة أكبر من قيمة F الجدولية واتضح وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية بين مراقبة إدارة المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى معنوية 0.05 واتضح أن المتغير المستقل (مراقبة إدارة المخاطر) يفسر 42.2 % من التغيرات التي تحدث في المتغير التابع (الحد من الهجمات السيبرانية) وأن باقي التغيرات ترجع لمتغيرات أخرى لم تدخل في النموذج وتبين أن كلما ازداد مستوى مراقبة إدارة المخاطر بمقدار 1 % ازداد مستوى الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية بمقدار 0.294 % مما يبين عدم صحة الفرضية الفرعية الثالثة للدراسة.

النتائج والتوصيات والمقترحات

نتائج الدراسة

- ✓ وجود مستوى مرتفع جدا من تحديد وتقييم المخاطر كأحد ابعاد إدارة مخاطر العامل البشري حيث بلغت قيمة المتوسط الحسابي 4.274 بانحراف معياري 0.712
- ✓ وجود مستوى مرتفع جدا من معالجة إدارة المخاطر كأحد ابعاد إدارة مخاطر العامل البشري حيث بلغت قيمة المتوسط الحسابي 4.297 بانحراف معياري 0.675
- ✓ وجود مستوى مرتفع جدا من مراقبة إدارة المخاطر كأحد ابعاد إدارة مخاطر العامل البشري حيث بلغت قيمة المتوسط الحسابي 4.340 بانحراف معياري 0.648
- ✓ وجود مستوى مرتفع جدا من كأحد ابعاد إدارة مخاطر العامل البشري حيث بلغت قيمة المتوسط الحسابي 4.297 بانحراف معياري 0.675
- ✓ ارتفاع مستوى الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية المحدودة حيث بلغت قيمة المتوسط الحسابي 4.095 بانحراف معياري 0.775.
- ✓ وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية بين إدارة مخاطر العامل البشري بأبعادها (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى معنوية 0.05 واتضح أن المتغير المستقل (إدارة مخاطر العامل البشري) يفسر 76.9 % من التغيرات التي تحدث في المتغير

التابع (الحد من الهجمات السيبرانية) وإن باقي التغيرات ترجع لمتغيرات أخرى لم تدخل في النموذج وتبين أن كلما ازداد مستوى إدارة مخاطر العامل البشري بمقدار 1 % ازداد مستوى إدارة مخاطر العامل البشري بأبعادها (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية بمقدار 0.446% مما يبين عدم صحة الفرضية الرئيسية للدراسة.

✓ وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية بين تحديد وتقييم المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى معنوية 0.05 واتضح أن المتغير المستقل (تحديد وتقييم المخاطر) يفسر 55.7 % من التغيرات التي تحدث في المتغير التابع (الحد من الهجمات السيبرانية) وإن باقي التغيرات ترجع لمتغيرات أخرى لم تدخل في النموذج وتبين أن كلما ازداد مستوى تحديد وتقييم المخاطر بمقدار 1 % ازداد مستوى للتخطيط الاستراتيجي على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية بمقدار 0.361% مما يبين عدم صحة الفرضية الفرعية الأولى للدراسة.

✓ وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية بين معالجة إدارة المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى معنوية 0.05 واتضح أن المتغير المستقل (معالجة إدارة المخاطر) يفسر 48.1 % من التغيرات التي تحدث في المتغير التابع (الحد من الهجمات السيبرانية) وإن باقي التغيرات ترجع لمتغيرات أخرى لم تدخل في النموذج وتبين أن كلما ازداد مستوى معالجة إدارة المخاطر بمقدار 1 % ازدادت الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية بمقدار 0.337 % مما يبين عدم صحة الفرضية الفرعية الثانية للدراسة.

✓ وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية بين مراقبة إدارة المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى معنوية 0.05 واتضح أن المتغير المستقل (مراقبة إدارة المخاطر) يفسر 42.2 % من التغيرات التي تحدث في المتغير التابع (الحد من الهجمات السيبرانية) وإن باقي التغيرات ترجع لمتغيرات أخرى لم تدخل في النموذج وتبين أن كلما ازداد مستوى مراقبة إدارة المخاطر بمقدار 1 % ازداد مستوى الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية بمقدار 0.294 % مما يبين عدم صحة الفرضية الفرعية الثالثة للدراسة.

✓ وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية بين على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى معنوية 0.05 واتضح أن المتغير المستقل (إدارة مخاطر العامل البشري) يفسر 48.1 % من التغيرات التي تحدث في المتغير التابع (الحد من الهجمات السيبرانية) وإن باقي التغيرات ترجع لمتغيرات أخرى لم تدخل في النموذج وتبين أن كلما ازداد مستوى بمقدار 1 % ازداد مستوى الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية بمقدار 0.337 % مما يبين عدم صحة الفرضية الفرعية الرابعة للدراسة.

التوصيات

- ✓ تعزيز برامج التوعية الأمنية المستمرة لجميع الموظفين، مع التركيز على التهديدات السيبرانية المرتبطة بالسلوك البشري كالهندسة الاجتماعية والتصيد الإلكتروني.
- ✓ تضمين إدارة مخاطر العامل البشري ضمن الخطة الاستراتيجية للأمن السيبراني في المؤسسات الحكومية لضمان معالجة التهديدات البشرية بشكل منهجي.
- ✓ تصميم اختبارات تقييم دورية للموظفين لقياس مدى التزامهم وفهمهم للسياسات الأمنية ومعايير حماية المعلومات.
- ✓ تفعيل أنظمة الرقابة والتحقق متعددة المستويات لضمان الكشف المبكر عن الأنشطة غير المصرح بها الناتجة عن خطأ أو سلوك بشري مقصود.
- ✓ دمج وحدات إدارة الموارد البشرية مع إدارات الأمن السيبراني لإيجاد بيئة عمل تدعم السلوك الأمني المسؤول والوقائي.
- ✓ تطبيق سياسة العقوبات والمكافآت لربط الالتزام بالإجراءات الأمنية بمستوى الأداء الوظيفي.
- ✓ تحديث السياسات الأمنية باستمرار لمواكبة التطورات التكنولوجية والتكتيكات الجديدة التي قد تستغل العامل البشري.
- ✓ تطوير سيناريوهات محاكاة للهجمات السيبرانية تتضمن عناصر بشرية لتدريب الموظفين على التصرف السليم في حال التعرض لمحاولات اختراق.
- ✓ إشراك الموظفين في تطوير إجراءات الأمن السيبراني لرفع مستوى الالتزام والإدراك بالمخاطر المحتملة.
- ✓ تعزيز ثقافة العمل الوقائي والتبليغ الفوري عن أي سلوك مشبوه من خلال قنوات رسمية ومؤمنة داخل المؤسسة.

المقترحات

- إجراء دراسات مقارنة بين القطاعات الحكومية والخاصة في المملكة لقياس الفروقات في مستوى إدارة مخاطر العامل البشري.
- توسيع الدراسة لتشمل الأقاليم الإدارية المختلفة في المملكة لرصد التباين الجغرافي في الاستجابة للمخاطر البشرية السيبرانية.
- اقتراح إنشاء وحدة مستقلة لإدارة مخاطر السلوك البشري في كل مؤسسة حكومية مرتبطة بوحدة الأمن السيبراني.
- تصميم منصة وطنية موحدة للتدريب على الأمن السيبراني موجهة لموظفي القطاع العام مع تركيز خاص على أخطاء العامل البشري.
- دراسة أثر التحفيز المالي والمعنوي على مدى التزام الموظفين بالسلوكيات الأمنية الصحيحة.
- البحث في العلاقة بين مستوى التعليم والتخصص الوظيفي ومدى الوعي بالمخاطر السيبرانية لدى الموظفين الحكوميين.
- اقتراح إطار وطني لإدارة مخاطر العامل البشري يعزز منسوب الحوكمة الإلكترونية على مستوى القطاع العام.
- إجراء دراسات طولية لقياس تطور تأثير البرامج التدريبية على سلوك الموظفين في مجال الأمن السيبراني.

قائمة المراجع

أولاً: المراجع باللغة العربية

1. أبو نصر، أشرف أحمد محمد، الكايد، وائل جمال عبدالكريم، و الرقاد، محمد عبدالكريم سالم. (2020). أثر التخطيط الاستراتيجي في إدارة المخاطر في البنوك التجارية الأردنية (رسالة ماجستير غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
2. باقر، وفاء جاسم علي عباس، ارتيمة، هاني جزاع عبدالكريم، و الهواري، سامر فواز. (2020). أثر إدارة المخاطر في إدارة المشاريع الهندسية: الدور الوسيط للثقافة المنظمة في الهيئة العامة للطرق والنقل البري في دولة الكويت (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
3. بني مصطفى، عبيدة محمد حسين، و العفيف، جمال حسن عيسى. (2022). أثر فاعلية نظم المعلومات المحاسبية في إدارة المخاطر المؤسسية: دراسة ميدانية على المصارف الإسلامية الأردنية (رسالة ماجستير غير منشورة). جامعة جرش، جرش.
4. الجمل، أسيل كمال ربحي، و العيطان، غيث ناصر محمد. (2023). أثر إدارة المخاطر على الأداء المالي للبنوك التجارية الأردنية (رسالة ماجستير غير منشورة). جامعة آل البيت، المفرق.
5. الحسني، عبدالله بن حمود بن محمد، و الخشالي، شاكر جار الله محمود. (2022). أثر التفكير الاستراتيجي في إدارة المخاطر: الدور المعدل للدعم المنظمي في شركات المقاولات العمانية (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
6. حفصي، أسماء، بن منصور، ملاك، و بن محمود، الحاج عرابة. (2022). أثر مخاطر إدارة الإمداد في المؤسسة في ظل جائحة كورونا: دراسة حالة شركة الطاسيلي للخدمات البترولية - منطقة إرارة 2 - حاسي مسعود (رسالة ماجستير غير منشورة). جامعة قاصدي مرباح - ورقلة، ورقلة.
7. الرواشدة، عبدالله محمد عبدالله، و الهلسة، رولى هاني سلمان. (2022). أثر قيادة الأعمال على إدارة المخاطر للمشاريع وفق نظام COSO (رسالة ماجستير غير منشورة). جامعة مؤتة، مؤتة.
8. الرواشدة، ينال عاطف سلام، و الشورة، عبدالله أحمد سليمان. (2022). أثر إدارة المخاطر في مرونة سلسلة التوريد: الدور المعدل للتمكين في شركة البوتاس العربية (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
9. زين، ياسمين إلياس عطا، و الشاعر، سوسن عبدالله حمد الله. (2023). أثر التجديد الاستراتيجي في إدارة المخاطر في شركات التأمين الأردنية (رسالة ماجستير غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
10. سلمونة، محمد ياسين محمد، و هماش، عبدالسلام أحمد إسماعيل. (2024). المسؤولية الدولية الناشئة عن الهجمات السيبرانية (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
11. الشوحة، ريم عبدالله فلاح، و الحياصات، حمدان محمد. (2020). أثر فاعلية التدقيق الداخلي في إدارة المخاطر المؤسسية: الدور الوسيط لنظم تخطيط موارد المنشأة (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
12. الصمادي، دعاء حسين أحمد، و الرواشدة، هاني علي عارف. (2023). أثر خصائص مجلس الإدارة على الإفصاح عن المخاطر المالية: الدور المعدل لجودة التدقيق الخارجي: دراسة تطبيقية على شركات الصناعية المدرجة في بورصة عمان (رسالة ماجستير غير منشورة). جامعة جرش، جرش.

13. العليمات، عبير عبدالله سليمان، و الشيخ، عماد يوسف أحمد أحمد. (2023). أثر إدارة المخاطر المؤسسية وفقاً لإطار "COSO" في الأداء المالي: الدور المعدل لجودة التدقيق الخارجي (رسالة ماجستير غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
14. العمري، نور محمد، و كلبونة، أحمد يوسف. (2022). أثر إدارة المخاطر الائتمانية في تحسين أداء البنوك التجارية الأردنية: حسب بطاقة الأداء المتوازن (رسالة ماجستير غير منشورة). جامعة البلقاء التطبيقية، السلط.
15. العنبرية، سارة بنت علي بن ناصر، و الجهاني، عبدالناصر السيد محمد. (2023). المسؤولية الدولية الجنائية عن الهجمات السيبرانية أثناء النزاعات المسلحة (رسالة ماجستير غير منشورة). جامعة السلطان قابوس.
16. عوض، راما محمود جوهر، و خشمان، أيسر محمد علي. (2022). أثر الذكاء الاستراتيجي في إدارة المخاطر في المستشفيات الخاصة الأردنية (رسالة ماجستير غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
17. القحطاني، محمد عبدالهادي ظافر العرجي، و أبو قاعود، غازي رسمي عايد. (2023). أثر القدرات الديناميكية في إدارة المخاطر السيبرانية: المرونة الاستراتيجية متغيراً وسيطاً: دراسة تطبيقية في وزارة الداخلية في دولة قطر (رسالة دكتوراه غير منشورة). جامعة مؤتة، مؤتة.
18. القحطاني، محمد عبدالهادي ظافر العرجي، و أبو قاعود، غازي رسمي عايد. (2023). أثر القدرات الديناميكية في إدارة المخاطر السيبرانية: المرونة الاستراتيجية متغيراً وسيطاً: دراسة تطبيقية في وزارة الداخلية في دولة قطر (رسالة دكتوراه غير منشورة). جامعة مؤتة، مؤتة.
19. المري، حمد سالم، القعيد، مرزوق عايد، و الصوالحة، أيوب أحمد محمد. (2020). أثر إدارة المخاطر على الأداء الاستراتيجي: نداء الأعمال كمتغير وسيط في البنوك التجارية العاملة في دولة الكويت (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
20. المعاينة، أسيل يحيى، و المخادمة، أحمد عبدالرحمن كريم. (2023). أثر إدارة المخاطر التشغيلية في دعم الميزة التنافسية: دراسة تطبيقية على البنوك التجارية العاملة في الأردن (رسالة ماجستير غير منشورة). جامعة مؤتة، مؤتة.
21. المقدشي، على حسين علي، و القرشي، عبدالله علي. (2019). أثر إدارة المخاطر المصرفية على ربحية البنوك اليمنية: دراسة مقارنة بين البنوك التجارية والإسلامية (رسالة ماجستير غير منشورة). جامعة الأندلس للعلوم والتقنية، صنعاء.
22. النجار، عمر محمد خليل، و الفراء، ماجد محمد عبدالسلام. (2019). أثر إدارة المخاطر على التميز المؤسسي لجامعة الأقصى بقطاع غزة (رسالة ماجستير غير منشورة). الجامعة الإسلامية (غزة)، غزة.

ثانياً: المراجع باللغة الإنجليزية

1. Abdul Jader, Ahmed Maysar. (2022). Factors Affecting the Behavioral Intention to Adopt Web-Based Recruitment in Human Resources Departments in Telecommunication Companies in Iraq. Anbar University Journal of Economic and Administrative Sciences, Vol. 14, No. 2, 404-416.
2. Abu Alead, R. M. S., and Ab Altalibe, A. A. (2023). Attribution Challenges in the Era of Cyber Warfare: Unraveling the Identity of Cyber-Attackers. Journal of the Higher Institute for Qualitative Studies, Vol. 3, No. 16, 5287-5309.

3. Abu Aliqa, Roaa Yousef, and Attir, Mohammed Abdullah Aref. (2023). An Enhanced Gazelle Optimization Algorithm for Intrusion Detection System in Wireless Sensor Networks (Unpublished Master's Thesis). Arab Open University, Amman.
4. Ahmed, Maqbool, Kazar, Aqaba, and Harous, Saad. (2024). Generative Artificial Intelligence for Cyber Security: Literature Review and Challenges. *Scientific Journal of Saba Region University*, Vol. 7, No. 2, 425-470.
5. Al-Amri, Samah Khaled Ibrahim, and Sweidan, Andraos Issa. (2019). Analysis and Synthesis of Efficient Intrusion Detection System in Internet of Things (Unpublished Master's Thesis). University of Jordan, Amman.
6. Al-Balawi, Khalaf bin Mohammed. (2025). Opportunities for Cyber Insurance to Address the Challenges of Cyber Attacks: Repercussions for SMEs. *University of Sharjah Journal of Legal Sciences*, Vol. 22, No. 1, 560-607.
7. Albalushi, J. K. J., Ali, S., and Aman, W. (2022). Proposed Enhanced Systematic Approach of Impact Analysis Process for Cyber-Attacks on Distributed Control Systems (Unpublished Master's Thesis). Sultan Qaboos University, Muscat.
8. Al-Dhawadi, Mahmoud Abdel Salam. (2020). The Third Human Dimension' Paradigm: A New Intellectual Framework for the Promotion of Cultural Sociology. *Journal of Arts*, Vol. 32, No. 1, 1-11.
9. Al-Masry, Baha Nayef Ismail, and Jaradat, Ghaith Mohammed. (2022). Sperm Swarm Optimization Algorithm for Intrusion Detection System in Wireless Sensor Networks (Unpublished Master's Thesis). Arab Open University, Amman.
10. Al-Muadat, Amna Awad, Bani Ahmed, Suleiman Ahmed, and Al-Durgham, Osama Mohammed Ahmed. (2023). Prediction of Cyber Attacks on the Cloud Computing Services for Big Data Applications (Unpublished Master's Thesis). Al-Balqa Applied University, As-Salt.
11. Al-Muadat, Amna Awad, Bani Ahmed, Suleiman Ahmed, and Al-Durgham, Osama Mohammed Ahmed. (2023). Prediction of Cyber Attacks on the Cloud Computing Services for Big Data Applications (Unpublished Master's Thesis). Al-Balqa Applied University, As-Salt.
12. Al-Quraan, Rabi' Sufyan Tayseer, and Obaidat, Ibrahim Muhammad Salem. (2023). Modeling and Simulation of New AI Technique to Address and Limit Cyber Attacks: ChatGPT Experimental Based (Unpublished Master's Thesis). Hashemite University, Zarqa.
13. Al-Ramadan, Bashayer Adnan, Shahid, Mohammed, Kapila, Kosem, and Al-Fadhli, Suad Mohammed. (2022). The Correlation of High-Risk Human Papillomavirus "HR-HPV" with Lesion Progression and other Risk Factors (Unpublished Master's Thesis). Arabian Gulf University, Manama.
14. Al-Salahi, Fatima Abdullah, and Al-Tarawneh, Alaa Al-Din Awad. (2024). Factors Affect Economic Well-Being: Human Developing Index for Selected Arab Countries. *Jordanian Journal of Economic Sciences*, Vol. 11, No. 1, pp. 24-34.
15. Al-Tamimi, Omar Ahmed, and Mughaid, Alaa Saeed Mohammed. (2024). A Novel Cyber Techniques for Detecting and Preventing Phishing Attacks Using AI (Unpublished Master's Thesis). Hashemite University, Zarqa.
16. Al-Tarawneh, Ghosoun Khalaf Firas, Al-Jubouri, Salloum Ahmed Dawood, and Al-Maaytah, Omar Nawaf Khaled. (2020). Impact of Human Factors on

- Quality Improvement of Production Systems (Unpublished Master's Thesis). Mutah University, Mutah.
17. Al-Zakwani, Alia Saeed, Zidoum, H. M., and Al-Hamadani, A. (2024). Phishing Attack Detection: A Comparative Study of Fully Connected Networks, Long Short Term Memory and Convolutional Neural Networks on the Eurepoc Dataset (Unpublished Master's Thesis). Sultan Qaboos University, Muscat.
 18. Attia, Zaid Ramzi Hashem, Obaidat, Maher Suleiman, and Al-Saghir, Maher Abdul-Moneim. (2024). Expression of Human Epidermal Growth Factor Receptor 2 "HER2" in Colorectal Cancer and its Correlation with Clinicopathological Characteristics among Jordanian Patients (Unpublished Master's Thesis). Al-Balqa' Applied University, As-Salt.
 19. Awad, Lana Nabil Hussein, and Al-Khazaali, Ziad Ali Fadl. (2022). Critical Factors that Affect the Adoption of Human Resource Information Systems "HRIS" in the International Organizations for Migration (Unpublished Master's Thesis). Al-Ahliyya Amman University, Salt.
 20. Badran, A., Abdel Gaber, S., and Haggag, R. (2024). Proposed Cyber Security Framework for Reducing the Security Risks on the Egyptian Petroleum Sector. *Scientific Journal of Business Research and Studies*, Vol. 38, No. 3, 1247-1301.
 21. Bouziane, S., and Latreche, T. (2025). Cyber Assurance and Cyber Risk Management: A Critical Analysis of the Leading Low-Cost Product in Algeria. *Journal of Contemporary Business and Economic Studies*, Vol. 8, No. 1, 310-332.
 22. Debbache, H. S. L. N., Roula, D., and Benfenatki, N. (2023). Factors Influencing the Clinical Internship: A Survey of 3rd Year Medical Students at the Faculty of Medicine of Constantine. *Horizons for Science Journal*, Vol. 8, No. 4, 216-225.
 23. Dohi, Surour Abdul-Hussein. (2024). The Web Graph on Page, Host and Cyber Attacks. *Journal of Sustainable Studies*, Vol. 6, Supplement, 1071-1099.
 24. Hamed, S. M. S. H. (2023). Social Factors and Dialect Variation: An Analysis of Age, Gender, and Social Class in Linguistic Practice. *North European Academic Peer Review Journal for Studies and Research*, Vol. 4, No. 21, 243-269.
 25. Ismail, H. S. G. (2020). Students' Cyber-Bullying of Secondary Schools Teachers as a Form of Social Exclusion in Saudi Arabia since the Outbreak of COVID-19. *Journal of the College of Education*, Vol. 78, No. 2, 65-111.
 26. Laib, S. (2021). The Importance of Cyber Security in the Financial Sector in the Age of Digital Transformation. *Al-Asil Journal of Economic and Administrative Research*, Vol. 5, No. 1, 448-464.
 27. Maqbul, M. Y. (2024). Factors Affecting Employees Motivation: An Exploratory Study of Employees at the General Administration of Education in Jeddah. *Arab Journal of Scientific Publishing*, No. 73, 71-96.
 28. Metwally, A. B. M., Abdelazim, S. I., and Almarji, M. T. (2022). Internal Auditors' Role In Confronting Cyber and Fraud Risks Related to Outsourcing Insurance: An Exploratory Study. *Alexandria Journal of Accounting Research*, Vol. 6, No. 3, 1-31.
 29. Ramadan, F. A. (2022). Outbreak Narratives and Medical Humanities: A Transdisciplinary Comparative Approach to the Literary Representation of

- Ebola in Preston's the Hot Zone (1994) and Tag Elsir's Ebola 76 (2012). College of Arts Journal, Volume 14, No. 2, 658-706.
30. Salim, A. T., and Khammas, B. M. (2023). Simplified Review on Cyber Security Threats Detection in IoT Environment Using Deep Learning Approach. Journal of the College of Basic Education, No. 119, 22-49.