

جامعة ميدأوشن

كلية الإدارة

تخصص إدارة المخاطر



دور الأمن السيبراني في إدارة مخاطر البيانات
لدى الشركات: دراسة تطبيقية على القطاع الخاص في المملكة العربية
السعودية

إعداد الطالب/عمر محمد عثماوي

243001793

إشراف/Rehab Elshafie

العام الدراسي:

2025

جدول المحتويات

2	مقدمة:
2	مشكلة الدراسة:
4	أهمية الدراسة:

أهداف الدراسة:	5
تساؤلات الدراسة	5
فروض الدراسة:	7
نموذج الدراسة	7
الدراسات السابقة:	7
المنطلقات النظرية للدراسة:	7
المنهجية وطرق البحث:	16
مصادر جمع البيانات	17
أدوات الدراسة :	18
حدود الدراسة :	18
المراجع:	19

مقدمة:

أصبح لزاماً على منظمات الأعمال في القرن الحادي والعشرين إتخاذ خطوات استباقية لاستشراف المستقبل وتطوير خططها الإبداعية المبنية على الحقائق والأدلة للتنبؤ بالمستقبل لاستغلال الفرص المتاحة والحد من آثار المخاطر التي قد تواجهها ؛ فالقيادات المتميزة القادرة على الاستغلال الأمثل للموارد المتاحة وتسخيرها لتقديم خدمات ومنتجات تفوق خدمات المنافسين أحد متطلبات النجاح لتحقيق النتائج المؤسسية المتميزة وتعزيز رضى أصحاب العلاقة لضمان استدامة أعمال تلك المنظمات وقدراتها التنافسية (Deaver-Vazquez et al., 2024) .

أصبحت إدارة الأمن السيبراني في المنظمات ذات أهمية كبيرة ومتزايدة في ظل الأزمات المتسارعة التي يمر بها العالم بدءاً من الهجمات السيبرانية على الحكومات والمنظمات وانتهاءً بالأفراد، مثل الهجمات الإلكترونية التي شنتها الولايات المتحدة عام 2019 على شبكة الكهرباء الروسية كرد على الإلكترونية عام 2017 على أحد مصانع شركة أرامكو السعودية، والهجمات التي تعرض لها بنك Flagstar الأمريكي من خلال نشر معلومات عن العملاء من قبل المخربين، ويذكر بأن أكثر من 2244 هجمة إلكترونية تحدث كل يوم بالعالم بتكلفة تتجاوز 11 تريليون دولار، وأن 71% من المنظمات في جميع أنحاء العالم هم ضحايا لتلك الهجمات بحسب ما نشرته مجلة إند بدنت

على موقعها بتاريخ 28/06/2022 ؛ وبناء على ما تقدم أضحت جميع المنظمات باختلاف قطاعاتها تبحث عن كيفية اكتشاف الهجمات السيبرانية وقياس مخاطرها والإبلاغ عنها وإدارتها ومجابهتها، وقد رسخت تلك المخاطر وآثارها السلبية الكبيرة ضرورة تطبيق النهج الاحترافي لإدارة الأزمات بفعالية وكفاءة للحد من تأثيرها ومواجهة عواقبها لضمان استقرار النظام الإداري والمالي للمنظمات واستدامة أعمالها وبقائها في السوق (Silva, 2024) إن المخاطر السيبرانية المتغيرة في سياقها وخصائصها وتأثيراتها قد يكون لها عواقب وخيمة على الشركات التي لا تمتلك الآليات المناسبة لمواجهتها (Kaushik, 2024)، فيما قد تعمل الشركات الرائدة على اقتناص ما تحتويه من فرص لتحويلها إلى قيمة مضافة لتعزيز أداءها وميزتها التنافسية (Ogborigbo et al., 2024) .

وتعد إدارة مخاطر البيانات عنصرًا حيويًا في استراتيجيات الحوكمة والأمن السيبراني، حيث تهدف إلى تحديد، تقييم، والتخفيف من المخاطر المرتبطة بجمع البيانات، تخزينها، معالجتها، ومشاركتها داخل المؤسسات، و تتزايد أهمية هذه الإدارة في ظل تصاعد التهديدات السيبرانية، حيث أصبحت الشركات أكثر عرضة للاختراقات الأمنية، هجمات الفدية، والتسريبات المعلوماتية، مما قد يؤدي إلى خسائر مالية جسيمة، تضرر السمعة، ومخاطر قانونية، وتعتمد إدارة مخاطر البيانات على إجراءات تحليلية واستباقية تشمل تطبيق أنظمة التشفير، المصادقة المتقدمة، والمراقبة المستمرة، لضمان سرية البيانات وسلامتها وتوافرها في بيئة تشغيلية آمنة (Silva, 2024).

في سياق التحول الرقمي، أصبحت المؤسسات مطالبة بالامتثال للوائح حماية البيانات مثل اللائحة العامة لحماية البيانات (GDPR) في أوروبا، ومعايير NIST و ISO 27001، لضمان حماية أصولها الرقمية وتعزيز ثقة العملاء والشركاء، ولا تزال العديد من المؤسسات تفتقر إلى نهج متكامل لإدارة المخاطر السيبرانية، مما يؤدي إلى تعرض بياناتها لمخاطر متزايدة نتيجة الإهمال أو عدم كفاية التدابير الأمنية، وتكمن أهمية إدارة مخاطر البيانات في توفير إطار تنظيمي متكامل يساعد المؤسسات على تحليل المخاطر المحتملة، تطوير خطط استجابة فعالة، وتعزيز ثقافة الأمن السيبراني بين الموظفين، مما يضمن استدامة العمليات التشغيلية وتقليل الخسائر الناجمة عن الحوادث السيبرانية (Deaver-Vazquez et al., 2024).

ونظرًا لأن الشركات تتجه بشكل متزايد نحو التحول الرقمي والاعتماد على التقنيات الحديثة، فإن تطوير إطار شامل لإدارة الأمن السيبراني يعد أمرًا ضروريًا لمواجهة التهديدات السيبرانية المتطورة، من خلال اعتماد استراتيجيات استباقية تشمل التحليل المستمر للمخاطر، تطبيق أحدث تقنيات الحماية، وتعزيز ثقافة الأمن السيبراني داخل المؤسسات. وقد أكدت الدراسات أن الشركات التي

تستثمر في الأمن السيبراني تحقق أداءً أفضل، زيادة في حصتها السوقية، وتحقيق أرباح أعلى في بيئة الأعمال العالمية التنافسية. (Olaniyi et al., 2023).

بناءً على ذلك، تهدف هذه الدراسة إلى استكشاف دور الأمن السيبراني بأبعاده المختلفة في إدارة مخاطر البيانات لدى المؤسسات الخاصة في المملكة العربية السعودية

مشكلة الدراسة:

في ظل التطور المتسارع للتقنيات الرقمية، أصبحت المؤسسات الخاصة أكثر عرضة للتهديدات السيبرانية، مما يفرض الحاجة إلى تعزيز استراتيجيات الأمن السيبراني لحماية البيانات وإدارة المخاطر بفعالية، ورغم الجهود المبذولة لا تزال العديد من الشركات تعتمد على أساليب تقليدية في حماية بياناتها، مما يجعلها غير مؤهلة للتعامل مع المخاطر المتزايدة والمتطورة (Deaver-Vazquez et al., 2024).

وتشير الدراسات إلى أن الأمن السيبراني لم يعد مجرد خيار تقني، بل أصبح عنصرًا حاسمًا في استدامة الأعمال، حيث تؤدي الاختراقات الأمنية إلى خسائر مالية كبيرة، وتراجع ثقة العملاء، ومخاطر قانونية بسبب عدم الامتثال للوائح حماية البيانات (Silva, 2024)، ولا تزال هناك فجوة في الأبحاث التي تربط بين أبعاد الأمن السيبراني المختلفة (أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات) وإدارة مخاطر البيانات، خاصة في بيئة الأعمال السعودية (Ogborigbo et al., 2024).

على الرغم من أن بعض الشركات بدأت في تبني تقنيات متقدمة مثل التشفير، المصادقة الثنائية، والمراقبة المستمرة، إلا أن مستوى الوعي والتنفيذ لهذه التدابير يختلف بشكل كبير بين المؤسسات، مما يعوق تحقيق أمن سيبراني شامل يحمي الأصول الرقمية بفعالية (Kaushik, 2024). كما أن غياب ثقافة أمنية قوية داخل المؤسسات يعزز من احتمالية وقوع الاختراقات، مما يستدعي دراسة أعمق حول كيفية دمج الأمن السيبراني في الهيكل التنظيمي للمؤسسات الخاصة (Olaniyi et al., 2023).

بناءً على ما سبق، تنبع مشكلة الدراسة من الحاجة إلى تقييم دور الأمن السيبراني بأبعاده المختلفة في إدارة مخاطر البيانات داخل المؤسسات الخاصة في المملكة العربية السعودية.

أهمية الدراسة:

تبرز أهمية هذه الدراسة من خلال تناولها لدور الأمن السيبراني في إدارة مخاطر البيانات في القطاع الخاص بالمملكة العربية السعودية، حيث تتزايد الحاجة إلى استراتيجيات قوية لحماية البيانات في ظل التهديدات السيبرانية المتصاعدة. تنقسم أهمية الدراسة إلى الجوانب التالية:

الأهمية العلمية:

- تساهم الدراسة في إثراء المعرفة العلمية حول العلاقة بين الأمن السيبراني وإدارة مخاطر البيانات، مما يساعد الباحثين والمتخصصين في تطوير فهم أعمق للموضوع.
- تسلط الضوء على أحدث الممارسات والتقنيات المستخدمة في الأمن السيبراني، مثل التشفير، والجدران النارية، وأنظمة الكشف عن الاختراقات، ودورها في الحد من المخاطر السيبرانية.
- تقدم إطارًا تحليليًا لتقييم مدى فعالية الأمن السيبراني في حماية البيانات وتقليل التهديدات في الشركات الخاصة.
- تساعد في سد الفجوة البحثية حول كيفية تأثير تطبيقات الأمن السيبراني على استدامة الأعمال في القطاع الخاص، خاصة في سياق الاقتصاد الرقمي المتنامي في المملكة العربية السعودية.
- توفر أساسًا للباحثين لإجراء دراسات مقارنة بين القطاعات المختلفة، وتحليل مدى تأثير التدابير الأمنية في تقليل المخاطر الرقمية على نطاق أوسع.

الأهمية العملية:

- توفر نتائج الدراسة إرشادات واضحة للمؤسسات الخاصة حول كيفية تعزيز استراتيجيات إدارة المخاطر السيبرانية وتحسين إجراءات الحماية.
- تساعد المؤسسات على تحديد نقاط الضعف في بنيتها التحتية الرقمية وتطوير خطط استجابة فعالة ضد التهديدات السيبرانية.
- تساهم في رفع وعي الشركات الخاصة بأهمية الامتثال للوائح التنظيمية المتعلقة بحماية البيانات، مثل معايير ISO 27001 والتشريعات الوطنية مثل نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية.
- تدعم الشركات في تحقيق ميزة تنافسية من خلال بناء ثقة العملاء وتعزيز سمعتها في السوق عبر تطبيق سياسات أمن سيبراني قوية.

أهداف الدراسة:

هدفت الدراسة إلى التعرف على دور الأمن السيبراني بأبعاده (أمن المعلومات، وأمن الشبكات، وأمن الإنترنت، وحماية البنية التحتية للمعلومات) في إدارة مخاطر البيانات لدى القطاع الخاص في المملكة العربية السعودية ، وتتفرع منها عدة أهداف فرعية منها :

- تحليل تأثير أمن المعلومات على تحسين إدارة مخاطر البيانات وتقليل احتمالية تسرب المعلومات في المؤسسات الخاصة.
- دراسة دور أمن الشبكات في تعزيز حماية البيانات داخل بيئات العمل الخاصة والحد من التهديدات السيبرانية التي تؤثر على إدارة المخاطر.
- تقييم مدى تأثير أمن الإنترنت على إدارة مخاطر البيانات، من خلال تحليل دور التقنيات الدفاعية في حماية البيانات من الاختراقات والهجمات الإلكترونية.
- استكشاف دور حماية البنية التحتية للمعلومات في تقليل المخاطر السيبرانية المرتبطة بتخزين البيانات ومعالجتها داخل القطاع الخاص.
- قياس مدى وعي المؤسسات الخاصة في المملكة العربية السعودية حول تأثير الأمن السيبراني على إدارة مخاطر البيانات ومدى التزامها بممارسات الحماية الرقمية.
- تحليل العلاقة بين تنفيذ استراتيجيات الأمن السيبراني ومستوى تقليل المخاطر المتعلقة بالبيانات وفقاً للمعايير والتشريعات الوطنية والدولية.
- اقتراح آليات واستراتيجيات لتحسين إدارة مخاطر البيانات من خلال تبني أحدث تقنيات الأمن السيبراني في الشركات الخاصة بالمملكة العربية السعودية.

تساؤلات الدراسة

السؤال الرئيسي: ما هو دور الأمن السيبراني بأبعاده المختلفة (أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات) في إدارة مخاطر البيانات لدى القطاع الخاص في المملكة العربية السعودية؟ ، وتتفرع منه عدة اهداف فرعية منها :

- كيف يؤثر أمن المعلومات على تقليل مخاطر تسرب البيانات في المؤسسات الخاصة؟
- ما هو دور أمن الشبكات في الحد من التهديدات السيبرانية وتحسين إدارة مخاطر البيانات؟
- كيف يساهم أمن الإنترنت في حماية البيانات وتقليل المخاطر الناجمة عن الهجمات الإلكترونية؟
- ما مدى تأثير حماية البنية التحتية للمعلومات على إدارة مخاطر البيانات واستمرارية الأعمال؟
- ما هو مستوى وعي المؤسسات الخاصة في المملكة العربية السعودية بأهمية الأمن السيبراني في إدارة مخاطر البيانات؟
- كيف يؤثر تنفيذ استراتيجيات الأمن السيبراني على مدى تقليل مخاطر البيانات وفقاً للمعايير والتشريعات الوطنية والدولية؟

- ما هي أفضل الآليات والاستراتيجيات المقترحة لتحسين إدارة مخاطر البيانات في القطاع الخاص من خلال تطبيق تقنيات الأمن السيبراني؟

فروض الدراسة:

لتحقيق أهداف الدراسة فقد أعتمد على مجموعة من الفرضيات الآتية:

الفرضية الرئيسية الأولى: يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لدور الأمن

السيبراني بأبعاده المختلفة (أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات) على إدارة مخاطر البيانات لدى القطاع الخاص في المملكة العربية السعودية، وينبثق من هذه الفرضية مجموعة من الفرضيات الفرعية التالية:

- يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لأمن المعلومات على إدارة مخاطر البيانات في المؤسسات الخاصة.
- يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لأمن الشبكات على تحسين إدارة مخاطر البيانات وتقليل التهديدات السيبرانية.
- يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لأمن الإنترنت على تقليل المخاطر السيبرانية وحماية البيانات من الهجمات الإلكترونية.
- يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لحماية البنية التحتية للمعلومات على تعزيز إدارة مخاطر البيانات وضمان استمرارية الأعمال.

الدراسات السابقة:

دراسة (Deaver-Vazquez et al., 2024)

هدف البحث إلى استكشاف دور تحديد المخاطر السيبرانية الكمية (CRQ) في تعزيز دقة وموضوعية إدارة المخاطر السيبرانية في الشركات الخاصة. يركز البحث على أهمية التقدير الرقمي لاحتمالية التهديدات وتأثيراتها المالية والتشغيلية، مما يساهم في توفير إطار عمل موحد لاتخاذ قرارات أكثر دقة

في مجال الأمن السيبراني. كما يتناول البحث أبعاد المخاطر السيبرانية الأساسية، مثل احتمالية وقوع الهجمات، وحجم التأثير على الأصول الرقمية، وفعالية استراتيجيات التخفيف، مع التركيز على قدرة CRQ على تحسين كفاءة تخصيص الموارد الأمنية وتقليل التحيزات الذاتية في عملية التقييم.

تعتمد الدراسة على منهج تحليل المخاطر الكمي من خلال دراسة تطبيقية على القطاع الخاص في المملكة العربية السعودية. تم جمع البيانات من عينة مكونة من عدد من الشركات الخاصة التي تعتمد استراتيجيات متنوعة في الأمن السيبراني، حيث تم تحليل بيانات المخاطر باستخدام نماذج كمية تعتمد على مؤشرات قابلة للقياس، مثل معدل حدوث الهجمات، التكاليف المحتملة للأضرار، وكفاءة استراتيجيات الاستجابة.

كشفت نتائج الدراسة أن استخدام النهج الكمي في تقييم المخاطر السيبرانية يعزز دقة اتخاذ القرارات، ويحسن الشفافية عند التواصل مع أصحاب المصلحة، ويقلل من عدم اليقين المرتبط بالأساليب التقليدية. كما أظهرت الدراسة أن الشركات التي تبنت CRQ تمكنت من تحسين استراتيجياتها الأمنية عبر تحديد أولويات المخاطر بناءً على التأثيرات الفعلية. بناءً على هذه النتائج، توصي الدراسة بضرورة اعتماد المؤسسات الخاصة في المملكة العربية السعودية لمنهجيات التقييم الكمي للمخاطر السيبرانية، وتعزيز ثقافة إدارة المخاطر المستندة إلى البيانات، وضمان تكامل الأمن السيبراني ضمن إطار إدارة المخاطر المؤسسية الشاملة.

دراسة (Silva, 2024)

هدفت الدراسة إلى تحليل التحديات القانونية والتنظيمية التي تنشأ عن الحوادث السيبرانية، مثل اختراق البيانات وهجمات الفدية وانتهاكات الأنظمة، وتأثيرها على الشركات والجهات التنظيمية، وتركز الدراسة على أبعاد متعددة، تشمل الالتزامات القانونية، المخاطر التنظيمية، الشفافية المؤسسية، وإدارة المخاطر السيبرانية، وتعتمد الدراسة على منهج تحليلي كمي ونوعي.

وأظهرت النتائج أن الأطر القانونية الحالية غير كافية لمعالجة الأضرار غير المالية، مما يزيد من مخاطر التقاضي ضد الشركات، خاصة في حال عدم الامتثال لممارسات إدارة المخاطر السيبرانية، كما كشفت الدراسة عن وجود نقص في الإفصاح عن المخاطر السيبرانية، على الرغم من المتطلبات القانونية.

بناءً على هذه النتائج، توصي الدراسة بضرورة تطوير أطر قانونية جديدة تتضمن الأضرار النفسية، تعزيز الشفافية المؤسسية في الإفصاح عن المخاطر السيبرانية، وزيادة تبني استراتيجيات استباقية

لإدارة المخاطر، مثل معايير NIST و AICPA، لتعزيز القدرة المؤسسية على مواجهة التهديدات السيبرانية بفاعلية.

دراسة (Ogborigbo et al., 2024)

هدفت الدراسة إلى تحديد استراتيجيات تعزيز الأمن السيبراني في أنظمة التحليل الذكي للأعمال (BI)، من خلال استكشاف الأساليب والتقنيات التي يمكن استخدامها لحماية البيانات وتقليل المخاطر السيبرانية، وتشمل الأبعاد التي تركز عليها الدراسة: تقنيات التشفير المتقدمة، المصادقة الثنائية، أنظمة المراقبة، وأثر ثقافة الأمن السيبراني داخل المؤسسات على الحماية الفعالة للبيانات، وتعتمد الدراسة على نهج بحثي مختلط .

أظهرت النتائج أن تطبيق الأمن السيبراني بشكل استراتيجي يؤدي إلى تحسين حماية البيانات، وتقليل مخاطر الاختراقات، وتعزيز ثقة العملاء، وضمان الامتثال للوائح. كما كشفت الدراسة أن المؤسسات التي تستثمر في تدابير مثل تقنيات التشفير الحديثة، المصادقة المتقدمة، والمراقبة المستمرة تتمتع بمستويات أمان أعلى، مما يقلل من الخسائر الناتجة عن الهجمات السيبرانية.

بناءً على هذه النتائج، توصي الدراسة بـ تطوير سياسات أمنية قوية، تدريب الموظفين على أساليب الأمن السيبراني، وتحديث الأنظمة بشكل دوري وفقًا لأحدث معايير الأمان مثل NIST و ISO 27001 لضمان استمرارية الأعمال وتعزيز مكانة المؤسسات في السوق.

دراسة (Kaushik, 2024)

هدفت الدراسة إلى تقديم منهجية شاملة مبتكرة لإعادة تعريف نهج المؤسسات في حماية أصولها المعلوماتية الحيوية، من خلال تنفيذ وتقييم استراتيجية متكاملة للأمن السيبراني، وتعتمد الدراسة على منهج تحليلي تطبيقي، حيث يتم دمج التحليلات المتقدمة، تقنية البلوك تشين، وخوارزميات التعلم الآلي لإنشاء نموذج أكثر دقة وقدرة على التنبؤ بالتهديدات السيبرانية والتعامل معها بفعالية، وتشمل العينة مجموعة متنوعة من المؤسسات التي تواجه تحديات أمنية مختلفة، حيث تم اختبار المنهجية المقترحة عبر تجارب ميدانية وتحليل بيانات الأمن السيبراني، لتقييم مدى فعاليتها في تعزيز قدرات الدفاع الرقمي. تم تحليل البيانات من خلال نماذج محاكاة المخاطر السيبرانية وأنظمة إدارة المعلومات الأمنية لتقييم كفاءة التدابير الوقائية وتحديد سبل تحسينها.

أظهرت النتائج أن تطبيق هذه المنهجية الشاملة يعزز وضع الأمن السيبراني للمؤسسات بشكل جذري، من خلال تحسين القدرات التعاونية، وزيادة المرونة الأمنية، وبناء بيئة سيبرانية متماسكة ومتطورة. كما بينت الدراسة أن التكامل بين التحليلات المتقدمة والذكاء الاصطناعي والتقنيات الحديثة يساهم في خفض احتمالات الاختراقات الأمنية، وتحسين الاستجابة للحوادث، وتعزيز استدامة استراتيجيات الأمن السيبراني.

بناءً على هذه النتائج، توصي الدراسة بـ اعتماد نهج أمني متكامل، يشمل تقنيات الذكاء الاصطناعي والبلوك تشين، وتعزيز ثقافة الأمن السيبراني داخل المؤسسات، وتطوير استراتيجيات استباقية لمواجهة التهديدات المستقبلية، لضمان حماية المعلومات وتحقيق مستويات أمان أعلى تتماشى مع تطورات العصر الرقمي.

دراسة (Olaniyi et al., 2023)

هدفت الدراسة إلى تحليل أهمية بناء ثقافة مخاطر قوية داخل المؤسسات لضمان نجاح استراتيجيات إدارة المخاطر المؤسسية (ERM) واستدامتها، وتعتمد الدراسة على نهج تحليلي تطبيقي يركز على تقييم تأثير العوامل التنظيمية والثقافية على نجاح إدارة المخاطر المؤسسية. تشمل العينة مجموعة من الشركات التي تعتمد ERM، حيث تم تحليل استراتيجياتها التنظيمية، ومستويات الشفافية، وتفاعل الموظفين مع سياسات المخاطر. كما تم قياس مدى تكامل إدارة المخاطر مع عناصر الحوكمة المؤسسية، التخطيط الاستراتيجي، تقييم الأداء، وتدفق المعلومات داخل المؤسسات.

كشفت النتائج أن بناء ثقافة مخاطر قوية داخل المؤسسات يساعد على تحقيق استدامة إدارة المخاطر المؤسسية (ERM)، ويؤدي إلى تحسين الحوكمة، وتعزيز عمليات اتخاذ القرار، وزيادة القدرة التنافسية. كما أظهرت الدراسة أن وضوح الأدوار، التواصل الشفاف، وإشراك الموظفين في عمليات إدارة المخاطر يساهم في التغلب على الحواجز التنظيمية وتحقيق نجاح طويل الأمد في ERM. بناءً على هذه النتائج، توصي الدراسة بدمج التقنيات الحديثة في إدارة المخاطر، تعزيز برامج التدريب والتوعية، وإنشاء قنوات اتصال فعالة بين جميع المستويات الإدارية لضمان استمرارية الأداء الفعال لأنظمة إدارة المخاطر المؤسسية.

دراسة (العبدالات والشورة، 2023)

هدفت الدراسة للتعرف الى أثر الأمن السيبراني بأبعاده تحديد (الأدوار والمسؤوليات ، أمن وسلامة المعلومات ، البنية التحتية الإلكترونية، تدريب العاملين) والتسويق الإلكتروني بأبعاده خدمات البنك الإلكترونية ، الترويج الإلكتروني ، التوزيع الإلكتروني ، إدارة علاقات العملاء الإلكترونية في البنوك التجارية الأردنية ، استخدمت الدراسة المنهج الوصفي التحليلي لتفسير الأثر بين متغيرات الدراسة و تم استخدام مجموعة من الأساليب الإحصائية التي تشتمل عليها الحزمة الإحصائية للعلوم الاجتماعية (SPSS) وذلك لغايات تحليل البيانات ، تم تطوير الاستبانة كأداة لجمع بيانات الدراسة استخدمت الدراسة على عينة العشوائية الطبقية التناسبية حيث بلغ حجم العينة (299) موظف وموظفة وجاءت ممثلة لجميع العاملين في أقسام التسويق وتكنولوجيا المعلومات في البنوك التجارية الأردنية في العاصمة عمان .

أظهرت النتائج وجود أثر للأمن السيبراني في التسويق الإلكتروني في البنوك التجارية الأردنية ، وفق متغيرات المستقل تحديد الأدوار والمسؤوليات ، امن وسلامة المعلومات والبيانات، البنية التحتية الإلكترونية ، تدريب العاملين وكانت النتائج الدراسة أن الأمن السيبراني يساهم في حماية الأنظمة الإلكترونية من الوصول أو الاستخدام أو الكشف غير المصرح ، ويعد الأمن السيبراني مهما في التسويق الرقمي في البنوك لأنه يساعد في حماية موقع الويب الخاص فيها عبر الأنترنت من التعرض للاختراق ، ضمان تحديد أدوار ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيقات وضوابط الأمن السيبراني يؤثر إيجابا على التسويق الإلكتروني.

ولقد أوصت الدراسة العمل على مواكبة العمل لتزويد العاملين في البنوك التجارية الأردنية بالتقنيات الحديثة بأمن المعلومات والفضاء السيبراني ، وتشجيع البنوك على التقييم المستمر للثغرات ونقاط الضعف في نظم المعلومات ثم إعداد كوادر بشرية مؤهلة ومتخصصة في الأمن السيبراني والاستفادة من التجارب الدولية في هذا المجال.

دراسة (الفلاح وآخرون، 2023)

هدفت الدراسة إلى التعرف على تطبيق معايير الأمان السيبراني وأثرها على أداء شركات الاتصالات في الأردن. بناءً على مراجعة الدراسات السابقة وتحليلها، ذلك من خلال استخدام المنهج الوصفي التحليلي وتوزيع استبانة على عينة من الموظفين والمديرين حيث تم تطوير نموذج يعتبر معايير إدارة الأمان السيبراني (أمن المعلومات، وأمن الشبكات، وأمن الإنترنت، وحماية البنية التحتية للمعلومات) كمتغيرات مستقلة، وأداء شركات الاتصالات الأردنية الفاعلية، الكفاءة الإنتاجية، الإبداع كمتغير تابع.

توصلت النتائج إلى أن تطبيق معايير الأمان السيبراني بشكل سليم يؤدي إلى أداء متميز للشركات الاتصالات، حيث يُسهم تحسين الإنتاجية، وزيادة الفاعلية، وتعزيز الكفاءة والتشجيع على الابتكار، وأظهرت نتائج الدراسة أن تطبيق معايير الأمان السيبراني يسهم في تحسين الإنتاجية، وزيادة الفاعلية، وتعزيز الكفاءة، وتشجيع على الابتكار في شركات الاتصالات في الأردن. توصل البحث إلى استنتاجاته بناءً على تحليل البيانات وفحص فرضيات الدراسة، وقدم توصيات عملية لتعزيز استخدام معايير الأمان السيبراني كأداة استراتيجية لتحسين أداء شركات الاتصالات في المستقبل.

دراسة (الحجايا والحباشة، 2023)

هدفت الدراسة إلى التعرف على أثر الثقافة التنظيمية على الأمن السيبراني في الحكومة الإلكترونية وزارة العدل أنموذجاً"، حيث تم استخدام المنهج الوصفي التحليلي وتم استخدام استبيان مكون من (28) فقره واعتماد تحليل الانحدار البسيط (Simple Linear Regression)، وتم التأكد من صدق الأداة وثباتها واستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية (SPSS) لتحليل البيانات. ويتكون مجتمع الدراسة من الموظفين العاملين في وزارة العدل، وتم أيضاً اختيار عينة من مجتمع الدراسة باستخدام الطريقة الطبقية التناسبية العشوائية، وتكونت العينة من (97) موظفاً عاملاً في وزارة العدل. وخلصت الدراسة إلى النتائج التالية:

تؤكد الدراسة أن تطبيق الثقافة التنظيمية بأبعادها وتطبيق الأمن السيبراني بأبعاده في الحكومة الإلكترونية في وزارة العدل - الأردن كان بدرجة موافقة عالية.

وتوصي الدراسة بتعزيز الشفافية والمساءلة والاحترام والمصادقية لدى موظفي الدوائر الحكومية الأردنية، وتوصي الدراسة بالإشارة إلى أهمية دور القادة في تشجيع ودعم الثقافة التنظيمية التي تركز على الأمن السيبراني، من خلال تحديد دور الأولويات وتوفير الموارد وتعزيز التوعية والتدريب.

دراسة (على وآخرون، 2023)

هدف البحث إلى تحليل أثر دعم دور المراجعة الداخلية على تعزيز أنظمة الأمن السيبراني. ولتحقيق هذا الهدف تم تقسيم البحث إلى شقين، الشق النظري لتأصيل موضوع البحث واستطلاع الجهود السابقة في هذا المجال، والشق الميداني لاختبار فروض البحث، وذلك من خلال قائمة استبيان كأحد الأساليب المقترحة لتجميع البيانات الأولية من عينة البحث، ولقد تم تصميمها بشكل مبسط ومختصر بقدر المستطاع والتي تتعلق بأثر دعم دور المراجعة الداخلية على تعزيز أنظمة الأمن السيبراني .

وقد توصلت نتائج البحث إلى وجود علاقة ذات دلالة إحصائية بين دعم دور المراجعة الداخلية وتعزيز أنظمة الأمن السيبراني.

دراسة (التونى، 2023)

هدف البحث إلى التعرف على "أثر وعى العملاء بالقرصنة الإلكترونية كأداة لتحقيق الأمن السيبراني في البنوك الحكومية بمحافظة بورسعيد مع اختبار العلاقة ميدانيا بين المتغيرين، ومعرفة مدى العلاقة بين أبعاد وعى العملاء بالقرصنة الإلكترونية، الأمن السيبراني من وجهة نظر عملاء البنوك. ، وقد اعتمدت الباحثة على أسلوب العينة العشوائية من البنوك الحكومية بمحافظة بورسعيد وذلك نظرا لكبر حجم مجتمع البحث فإن أسلوب الحصر الشامل في جميع البيانات الخاصة بالبحث سيكون أمر صعب جدا لاعتبارات الوقت والجهد والتكلفة، وقد استخدمه أداة دراسة متمثلة في "استبانة"، واستند البحث على "المنهج الوصفي" ، وتكون مجتمع البحث من العملاء بالبنوك الحكومية بمحافظة بورسعيد وتم توزيع (450) واستخدام برنامج التحليل الإحصائي (SPSS) للإجابة عن أسئلة البحث، وخلصت لمجموعة من النتائج كان أبرزها بأن مستوى ودور إدارة الحماية البنكية كان مرتفعا، وكذلك بينت البحث وجود دور الأمن السيبراني بدلالة أبعاده (الجهود التنظيمية، المتطلبات الفنية، التنسيق مع المؤسسات الأخرى، رصد وتقييم التهديدات) في التوعية والحد من الجرائم المالية، أظهرت نتائج التحليل الإحصائي بأن فاعلية إجراء الرقابة الداخلية في توفير الأمن السيبراني في التصدي للجرائم (القرصنة الإلكترونية) وذلك من خلال توفير آليات مناسبة لتطوير معارف ومهارات للعملاء الحاليين والمستقبليين ورفع مستوى الوعي والإرشاد وتمكينهم من فهم المخاطر الأساسية للمعاملات التي يجرونها مع البنوك والتصدي من عمليات الاحتيال التي يعرض لها العملاء وكيفية توفير وتوضيح الطرق التي من خلالها يقوم المحتالون بخداع ضحاياهم .

أوصت الدراسة بضرورة تضافر الجهود بين القطاعات الحكومية ومن ضمنها البنوك في التعاون والتنسيق فيما بينها لأجل تطوير وتحسين إدارة الأمن السيبراني والقدرة علي توفير الثقافة البنكية ودورها في تحقيق التوعية المصرفية والتصدي للقرصنة الإلكترونية بالإضافة إلي زيادة الأبحاث المرتبطة بالأمن السيبراني إذ تبين قلة في هذه الدراسات وخصوصا العربية منها.

دراسة (الغامدى ووالمستادى، 2021)

هدفت الدراسة إلى التعرف على دور الأمن السيبراني في تحقيق الميزة التنافسية من خلال بحث وتحليل البرامج التي يقوم باستخدامها الموظفين والمستفيدين وتحديد دور الأمن السيبراني فيها وتغطية الفجوة العلمية في هذا المجال، وتم استخدام المنهج الوصفي التحليلي، حيث تم استخدام الاستبانة

لاستطلاع عينة البحث بهدف جمع البيانات، وتكون مجتمع البحث من الموظفين الإداريين بمطار الملك عبد العزيز الدولي بجدة حيث تم اختيار عينة عشوائية بسيطة مقدارها (340) موظف .

وتوصلت نتائج الدراسة إلى وجود دور إيجابي وبدرجة كبيرة في تحقيق الميزة التنافسية بمطار الملك عبد العزيز الدولي، ووجود علاقة عكسية ذات أثر سلبي بين توفر الخصوصية في مطار الملك عبد العزيز وتحقيق الميزة التنافسية، ووجود علاقة طردية ذات أثر موجب وأن التعزيز كمتغير مستقل يؤثر في تحقيق الميزة التنافسية، وكشفت نتائج الدراسة أن الميزة التنافسية تتحقق بدرجة كبيرة في مطار الملك عبد العزيز الدولي، وأوصت الباحثة بضرورة الاستمرار في تحقيق درجة عالية في مستوى الأمن السيبراني في مطار الملك عبد العزيز بجدة من خلال أبعاده (السرية، الخصوصية، والتعزيز)، حيث إن ذلك يعتبر جزءاً من الأمن الوطني للمملكة العربية السعودية، وذلك لأن أمن المعلومات الآن أصبح جزءاً أصيلاً في مجال علوم الأمن، ومراجعة أوجه الخلل في عناصر الخصوصية.

الفجوة البحثية

على الرغم من الاهتمام المتزايد بالأمن السيبراني ودوره في إدارة مخاطر البيانات، إلا أن الدراسات السابقة لا تزال تقتصر إلى تحليل متكامل يجمع بين جوانب الأمن السيبراني المختلفة (أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات) وتأثيرها على إدارة مخاطر البيانات في القطاع الخاص في المملكة العربية السعودية. ركزت الأبحاث السابقة على أحد هذه الأبعاد بشكل منفصل أو في سياقات محددة، مثل البنوك، شركات الاتصالات، أو المؤسسات الحكومية، دون تقديم نموذج شامل يوضح الترابط بين هذه العناصر داخل البيئة التجارية الخاصة في المملكة.

كما أظهرت الدراسات السابقة اهتماماً بالمعايير القانونية والتنظيمية، مثل دراسة Silva (2024) التي تناولت الأطر القانونية والتحديات التنظيمية للحوادث السيبرانية، لكنها لم تستكشف بشكل كافٍ كيف يمكن للقطاع الخاص في المملكة العربية السعودية موازنة استراتيجيات الأمن السيبراني مع هذه اللوائح لضمان الامتثال والحد من المخاطر القانونية. بالإضافة إلى ذلك، لم تتعمق الأبحاث في كيفية تأثير البيئة القانونية على تطبيق الأمن السيبراني بشكل عملي داخل المؤسسات الخاصة، وما إذا كان هناك التزام حقيقي من الشركات بتلك القوانين أو مجرد امتثال شكلي.

على صعيد آخر، ركزت دراسات مثل Deaver-Vazquez et al (2024) على النهج الكمي لتحديد المخاطر السيبرانية (CRQ)، وأكدت أن هذا الأسلوب يعزز دقة اتخاذ القرار وتقليل التحيزات الذاتية.

ومع ذلك، فإن هذه الدراسة لم تتناول بشكل كافٍ كيفية دمج CRQ مع استراتيجيات الأمن السيبراني التقليدية، مما يترك فجوة بحثية حول مدى توافق التحليل الكمي مع الحلول الأمنية الفعلية المستخدمة في المؤسسات الخاصة، وخاصة في المملكة العربية السعودية حيث تختلف التحديات السيبرانية بناءً على طبيعة السوق المحلي والبنية التحتية الرقمية.

كما أن الدراسات مثل Ogborigbo et al (2024) التي تناولت الأمن السيبراني في أنظمة التحليل الذكي للأعمال (BI) تركزت على التكنولوجيا الحديثة مثل التشفير المتقدم، المصادقة الثنائية، والمراقبة المستمرة، لكنها لم توضح كيف يمكن لهذه التقنيات أن تندمج في نموذج متكامل للأمن السيبراني وإدارة المخاطر في بيئات الأعمال المختلفة. من هنا، تبرز الحاجة إلى دراسة تربط بين الحلول التقنية الحديثة والاحتياجات الأمنية الواقعية في المؤسسات الخاصة بالمملكة.

ومن منظور أكثر شمولية، تناولت دراسة Kaushik (2024) منهجية جديدة في الأمن السيبراني من خلال تقنيات البلوك تشين والذكاء الاصطناعي، لكنها لم تتطرق إلى مدى قابلية تطبيق هذه المنهجية في الشركات الخاصة السعودية، خاصة مع التحديات الفعلية التي قد تواجهها تلك الشركات عند تبني هذه التقنيات، سواء من ناحية التكاليف أو من ناحية التوافق مع البنية التحتية المتاحة. لذا، فإن البحث في كيفية دمج الحلول التقنية الحديثة مع واقع الأمن السيبراني في القطاع الخاص السعودي يمثل فجوة بحثية تستحق الدراسة.

أخيراً، ركزت بعض الأبحاث مثل Olaniyi et al (2023) على ثقافة المخاطر في المؤسسات ودورها في استدامة إدارة المخاطر، لكن لم يتم ربط هذا المفهوم مع عوامل الأمن السيبراني، مما يجعل هناك حاجة لدراسة توضح كيف يمكن تعزيز ثقافة الأمن السيبراني في القطاع الخاص وتأثيرها على إدارة المخاطر السيبرانية بشكل فعال. في ظل بيئة الأعمال السعودية التي تشهد تطورات رقمية سريعة، لا يزال من غير الواضح مدى إدراك الشركات لأهمية ثقافة الأمن السيبراني، وكيفية دمجها في عملياتها اليومية للحماية من التهديدات السيبرانية.

تكشف الفجوة البحثية عن غياب دراسة متكاملة تستكشف العلاقة بين جميع أبعاد الأمن السيبراني وإدارة مخاطر البيانات في القطاع الخاص السعودي، مع التركيز على الجوانب القانونية، التكامل بين التقنيات الحديثة والممارسات التقليدية، والتحديات الفعلية التي تواجه المؤسسات في تطبيق استراتيجيات الأمن السيبراني. من هنا، تأتي أهمية هذه الدراسة لسد هذه الفجوة وتقديم نموذج شامل يعالج هذه القضايا بعمق.

المنطلقات النظرية للدراسة:

الأمن السيبراني (Cybersecurity):

يشير الأمن السيبراني إلى مجموعة من التقنيات، العمليات، والممارسات المصممة لحماية الشبكات، الأجهزة، البرامج، والبيانات من الهجمات السيبرانية أو الوصول غير المصرح به. يهدف إلى ضمان سرية، سلامة، وتوافر المعلومات، ويتضمن عدة أبعاد رئيسية تشمل أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات (Deaver-Vazquez et al., 2024).

إجرائيا : يتم قياسه من خلال درجة تطبيق المؤسسات الخاصة في المملكة العربية السعودية للإجراءات الأمنية المتعلقة بحماية المعلومات، الشبكات، الإنترنت، والبنية التحتية الرقمية. يتم جمع البيانات باستخدام استبيانات ومقاييس كمية تقيس مدى تبني هذه المؤسسات لتقنيات الأمان السيبراني والاستراتيجيات الوقائية.

أمن المعلومات (Information Security):

هو مجموعة من السياسات والإجراءات التي تركز على حماية البيانات من الوصول غير المصرح به، التلاعب، أو الضياع، مع الحفاظ على سريتها وسلامتها وتوافرها. يشمل أمن المعلومات تقنيات مثل التشفير، أنظمة التحكم في الوصول، وبرامج الحماية من الفيروسات (Ogborigbo et al., 2024).

إجرائيا : يتم قياسه من خلال عدد الإجراءات الأمنية المتبعة لحماية البيانات داخل المؤسسات، مثل استخدام التشفير، سياسات التحكم في الوصول، وآليات حماية البيانات الحساسة.

أمن الشبكات (Network Security):

يشير إلى التدابير المستخدمة لحماية الشبكات الداخلية والخارجية من الاختراقات والتسلل غير المصرح به، وذلك من خلال أنظمة الجدران النارية، بروتوكولات التشفير، وأنظمة كشف التسلل. يهدف أمن الشبكات إلى تأمين الاتصال بين الأنظمة المختلفة ومنع الهجمات الضارة (Kaushik, 2024).

إجرائيا : يتم قياسه من خلال مدى تبني المؤسسات لأنظمة الحماية الشبكية مثل الجدران النارية، أنظمة كشف التسلل، وتأمين نقاط الاتصال الداخلية والخارجية.

أمن الإنترنت (Internet Security):

يُعرف بأنه حماية الأنظمة المتصلة بالإنترنت من التهديدات الإلكترونية مثل الفيروسات، التصيد الاحتيالي، وهجمات البرمجيات الخبيثة. يتضمن هذا البعد استخدام تقنيات الأمان المتقدمة مثل تصفية المحتوى، برامج مكافحة الفيروسات، وأنظمة إدارة الهوية والمصادقة (Olaniyi et al., 2023).
إجرائيا : يتم قياسه من خلال عدد التدابير المتبعة لحماية العمليات الرقمية عبر الإنترنت، مثل برامج مكافحة الفيروسات، الحماية من التصيد الاحتيالي، والمصادقة الثنائية.

حماية البنية التحتية للمعلومات (Information Infrastructure Protection):

يشير إلى التدابير الأمنية المتخذة لحماية الأنظمة والموارد التقنية الأساسية التي تدعم العمليات الرقمية للمؤسسات، مثل مراكز البيانات، الخوادم، وأنظمة التخزين السحابية. يهدف هذا البعد إلى تقليل تأثير الهجمات السيبرانية على استمرارية الأعمال (الحجايا والحباشة، 2023).
إجرائيا : يتم قياسها من خلال مدى قدرة المؤسسات على تأمين أصولها الرقمية الأساسية مثل الخوادم، أنظمة النسخ الاحتياطي، ومراكز البيانات، باستخدام تقنيات التشفير، أنظمة التحكم في الوصول، وخطط استمرارية الأعمال.

إدارة مخاطر البيانات (Data Risk Management):

تُعرف إدارة مخاطر البيانات بأنها مجموعة من العمليات والسياسات التي تهدف إلى تحديد، تقييم، والتخفيف من المخاطر المرتبطة بجمع البيانات، تخزينها، نقلها، ومعالجتها. تهدف هذه العملية إلى تقليل احتمالية حدوث تسريبات أو اختراقات وضمان الامتثال للمعايير القانونية والتنظيمية (Silva, 2024).

إجرائيا : يتم تقييمها بناءً على مدى قدرة الشركات على تحديد المخاطر المرتبطة بالبيانات، تصنيفها وفق درجة الخطورة، وتطبيق خطط استجابة فعالة في حال وقوع اختراقات. يشمل القياس مدى الامتثال لمعايير الأمان، إجراءات الحماية المطبقة، وعدد الحوادث الأمنية المسجلة خلال فترة الدراسة.

المنهجية وطرق البحث:

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي، وهو منهج يستخدم لجمع وتحليل البيانات بطريقة منظمة لتفسير الظواهر ودراستها بشكل دقيق. يتميز هذا المنهج بالتركيز على وصف خصائص الظاهرة المدروسة، وتحليل العلاقات بينها وبين المتغيرات الأخرى، ومن ثم تفسير النتائج بناءً على البيانات التي

تم جمعها، و يتيح هذا المنهج فهم الظواهر كما هي موجودة في الواقع دون التدخل فيها، مما يجعله مثاليًا لدراسة تأثير الأمن السيبراني على إدارة مخاطر البيانات في القطاع الخاص.

مصادر جمع البيانات

تعتمد هذه الدراسة على المصادر الأولية كمصدر رئيسي لجمع البيانات، حيث سيتم استخدام الاستبيان كأداة وحيدة لجمع المعلومات مباشرة من المشاركين في الدراسة. سيتم تصميم الاستبيان بطريقة منهجية تغطي جميع المتغيرات الرئيسية للدراسة، مثل أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات، وذلك بهدف قياس تأثير الأمن السيبراني على إدارة مخاطر البيانات في المؤسسات الخاصة بالمملكة العربية السعودية، وسيتم توزيع الاستبيان على عينة من العاملين في أقسام تقنية المعلومات والأمن السيبراني داخل الشركات الخاصة، لضمان الحصول على بيانات دقيقة تعكس واقع الممارسات الأمنية في تلك المؤسسات.

أما المصادر الثانوية، فسيتم الاعتماد عليها لدعم تحليل النتائج وإثراء الإطار النظري للدراسة، حيث سيتم الرجوع إلى الدراسات السابقة، الكتب العلمية، التقارير المتخصصة، والمقالات الأكاديمية التي تتناول موضوع الأمن السيبراني وإدارة مخاطر البيانات، وستساعد هذه المصادر في توفير خلفية نظرية متينة، وتوضيح مدى توافق نتائج الدراسة الحالية مع نتائج الأبحاث السابقة، مما يساهم في تفسير النتائج المستخلصة من الاستبيان بشكل أكثر دقة وعمق.

أدوات الدراسة:

ستعتمد هذه الدراسة على أداة الاستبيان كأداة رئيسية لجمع البيانات الأولية من المشاركين. تم تصميم الاستبيان بطريقة علمية ومنهجية لضمان قياس دقيق لمتغيرات الدراسة، حيث يشمل مجموعة من الأسئلة التي تغطي أبعاد الأمن السيبراني الأربعة (أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات)، ومدى تأثيرها على إدارة مخاطر البيانات في المؤسسات الخاصة بالمملكة العربية السعودية.

وسيتم تطوير الاستبيان وفقًا لمقاييس علمية مستخدمة في الدراسات السابقة، مع مراعاة وضوح الأسئلة وسهولة الإجابة عليها لضمان جمع بيانات دقيقة وموضوعية. سيتم استخدام مقياس ليكرت الخماسي لقياس استجابات المشاركين، مما يسمح بتحليل اتجاهاتهم نحو تطبيق ممارسات الأمن السيبراني وتأثيرها على تقليل المخاطر السيبرانية.

الأساليب الإحصائية المستخدمة

تعتمد هذه الدراسة على مجموعة من الأساليب الإحصائية الكمية لتحليل البيانات المستخلصة من الاستبيان، وذلك باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية (SPSS) لضمان دقة النتائج واستخلاص استنتاجات علمية موثوقة. تشمل الأساليب الإحصائية المستخدمة ما يلي:

الإحصاء الوصفي (Descriptive Statistics):

يتم استخدام المتوسطات الحسابية، الانحراف المعياري، والنسب المئوية لوصف خصائص العينة، وتحليل استجابات المشاركين حول دور الأمن السيبراني في إدارة مخاطر البيانات.

اختبار الصدق والثبات (Reliability and Validity Tests):

يتم اختبار الصدق (Validity) للتأكد من أن الاستبيان يقيس المفاهيم المستهدفة بدقة.

يتم اختبار الثبات (Reliability) باستخدام معامل كرونباخ ألفا (Cronbach's Alpha) لقياس مدى اتساق إجابات المشاركين والتأكد من موثوقية الأداة البحثية.

تحليل الارتباط (Correlation Analysis):

يستخدم معامل ارتباط بيرسون (Pearson Correlation) لقياس العلاقة بين أبعاد الأمن السيبراني (أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات) ومستوى إدارة مخاطر البيانات.

تحليل الانحدار البسيط والمتعدد (Simple and Multiple Regression Analysis):

يتم تطبيق تحليل الانحدار البسيط لدراسة تأثير كل بعد من أبعاد الأمن السيبراني على إدارة مخاطر البيانات بشكل منفرد، ويتم استخدام تحليل الانحدار المتعدد لتحديد الأثر المجمع لجميع الأبعاد على المتغير التابع (إدارة مخاطر البيانات)، مما يساعد في فهم العوامل الأكثر تأثيراً.

حدود الدراسة:

← **حدود موضوعية:** تركز الدراسة على دور الأمن السيبراني بأبعاده المختلفة (أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات) في إدارة مخاطر البيانات في القطاع الخاص.

← **حدود زمنية:** سيتم إجراء الدراسة خلال الفترة 2024 إلى 2025 م .

← **حدود مكانية:** تقتصر الدراسة على المؤسسات الخاصة في المملكة العربية السعودية.

← **الحدود البشرية:** ستركز الدراسة على العاملين في أقسام تقنية المعلومات والأمن السيبراني داخل المؤسسات الخاصة في المملكة العربية السعودية، بما في ذلك مديرو أمن المعلومات، مسؤولو الشبكات، محللو البيانات، ومديرو المخاطر والامتثال، حيث يمتلكون الخبرة في تطبيق استراتيجيات الأمن السيبراني وإدارة مخاطر البيانات..

المراجع :

- التوني، شريهان مصطفى محمد. (2023). أثر وعي العملاء بالقرصنة الإلكترونية كأداة لتحقيق الأمن السيبراني: دراسة ميدانية على البنوك الحكومية بمحافظة بورسعيد. مجلة التجارة والتمويل، ع4، 609 - 653.
- الحجايا، ميرفت محمد فلاح، و الحباشنة، عبادة يوسف عبدالله. (2023). أثر الثقافة التنظيمية على الأمن السيبراني في الحكومة الإلكترونية الأردنية: وزارة العدل أنموذجاً (رسالة ماجستير غير منشورة). جامعة مؤتة، مؤتة.
- العبدلات، صدام عبدالله الكريم، و الشورة، محمد سليم خليف. (2023). أثر الأمن السيبراني في التسويق الإلكتروني في البنوك التجارية الأردنية (رسالة ماجستير غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
- علي، هيام عيد عطية محمد، دياب، محمد عبدالقادر، و عباس، حنان جابر حسن. (2023). أثر دعم دور المراجعة الداخلية على تعزيز أنظمة الأمن السيبراني: دراسة ميدانية. الفكر المحاسبي، مج27، ع4، 71 - 120.
- الغامدي، عهود أحمد، و المستادي، ولاء عبدالله. (2021). دور الأمن السيبراني في تحقيق الميزة التنافسية: دراسة ميدانية على موظفي مطار الملك عبدالعزيز الدولي بجدة. مجلة العلوم الاقتصادية والإدارية والقانونية، مج5، ع9، 144 - 164.
- الفلاح، حسام محمد سليمان، النصور، مروان محمد، و العربيات، أيمن عبدالهادي. (2023). أثر تطبيق معايير الأمن السيبراني على أداء شركات الاتصالات الأردنية (رسالة ماجستير غير منشورة). جامعة البلقاء التطبيقية، السلط.
- Deaver-Vazquez, C., Taylor, E., Rowley, D., & Langis, B. (2024). A QUANTITATIVE APPROACH TO ASSESSING AND MANAGING CYBERSECURITY RISKS. EDPACS, 69(4), 7-11.
- Kaushik, M. (2024). Cybersecurity Management: Developing Robust Strategies for Protecting Corporate Information Systems. International Journal for Global Academic & Scientific Research, 3(2), 24–35. <https://doi.org/10.55938/ijgasr.v3i2.75>
- Ogborigbo, J. C., Sobowale, O. S., Amienwalen, E. I., Owoade, Y., Samson, A. T., & Egerson, J. (2024). Strategic integration of cyber

security in business intelligence systems for data protection and competitive advantage. *World Journal Of Advanced Research and Reviews*, 23(1), 081–096. <https://doi.org/10.30574/wjarr.2024.23.1.1900>

- Olaniyi, O. O., Olabanji, S. O., & Abalaka, A. (2023). Navigating risk in the modern business landscape: Strategies and insights for enterprise risk management implementation. *Journal of Scientific Research and Reports*, 29(9), 103-109
- Silva, J. F. (2024). Navigating cybersecurity challenges: Legal implications and organizational strategies. *International Seven Multidisciplinary Journal*, 2(1). <https://doi.org/10.56238/isevmjv2n1-012>

Mid-Ocean University

College of Management

Specialization: risk mangement



**The Role of Cybersecurity in
Managing Data Risks in Companies: An Applied Study
on the Private Sector in the Kingdom of Saudi Arabia**

Preparation:

Omar Mohammed Eshmawi

243001793

Supervisor :

Dr. Rehab Elshafie

1446-2025