

جامعة ميدأوشن

كلية الإدارة

قسم / تخصص إدارة أعمال



عنوان البحث

الاستراتيجيات الفعالة لإدارة المخاطر والتخفيف منها في مجال أمن الشركات
في المملكة العربية السعودية

" Effective Strategies for Risk Management and Mitigation in the
Field of Corporate Security in the Kingdom of Saudi Arabia"

إعداد الطالب/ خالد عبده خبراني

الرقم الجامعي / 241000762

الدكتور المشرف/ د. أسماء أبو عنزه

العام الدراسي:

2024



شكر وتقدير

الحمد لله والشكر له كما ينبغي لجلال وجهه وعظيم سلطانه، عدد خلقه ورضا نفسه وزنة عرشه ومداد كلماته، على أن من علي بإنجاز هذه الدراسة والرسالة، والصلاة والسلام على أفضل الخلق نبينا محمد وعلى آله وصحبه وسلم تسليما كثيرا.

أتوجه بالشكر لجامعة/MIDOCEAN متمثلة في معالي مدير الجامعة وعميد الدراسات العليا وأتوجه بالشكر للمشرف على الرسالة، الدكتور أسماء أبو عنزه ، التي كان بعد الله - عز وجل- المعين الأول لي على إتمام هذه الدراسة، فلها كل الشكر والامتنان. والشكر موصول لصاحبي السعادة اللذين تفضلا بتحكيم خطة الدراسة ، ، وأتوجه بالشكر للسادة المحكمين لإسهامهم برأيهم وعلمهم في تحكيم أدوات الدراسة. وأتوجه بالشكر للسادة المناقشين، وأتوجه بالشكر والتقدير للقائمين على إخراج المناقشة، وفي مقدمتهم عمادة الدراسات الجامعية، وأتوجه بالشكر والتقدير لكل من قدم المساعدة خلال مراحل إعداد هذه الدراسة.

فهرس المحتويات

3	شكر وتقدير
5	المقدمة:
7	مشكلة الدراسة:
10	أهمية الدراسة:
13	أهداف الدراسة:
15	تساؤلات الدراسة
16	فروض الدراسة:
19	الدراسات السابقة:
22	المنطلقات النظرية للدراسة:
28	المنهجية وطرق البحث:
29	أدوات الدراسة :
30	حدود الدراسة :
32	المراجع:

المقدمة:

تعتبر إدارة المخاطر في الشركات مجالا حيويًا ، لا سيما في المملكة العربية السعودية حيث يشهد السوق تنوعًا وتطورًا مستمرين. يواجه القطاع الخاص مجموعة من التحديات التي تشمل المخاطر المالية، التشغيلية، الأمنية، والسيبرانية. تتطلب هذه التحديات تطبيق استراتيجيات فعالة لإدارة المخاطر تضمن استمرارية الأعمال وحمايتها من التهديدات المحتملة. تتضمن إدارة المخاطر عملية منهجية لتحديد وتحليل وتقييم المخاطر، ثم وضع خطط للتخفيف من آثارها والتحكم فيها، إن الخطوة الأولى في إدارة المخاطر هي التقييم الشامل. يشمل هذا التقييم تحديد جميع المخاطر المحتملة التي قد تواجهها الشركة وتحليل تأثيرها المحتمل، وبعد تحديد المخاطر، يتم وضع خطط وقائية لمواجهتها قبل أن تتحول إلى أزمات. تشمل هذه الخطط وضع سياسات وإجراءات للتعامل مع الحوادث الأمنية والطوارئ. كما يتم تطوير خطط استجابة سريعة للتعامل مع الأزمات عند وقوعها، مما يضمن استمرارية العمل وتقليل الخسائر.

تعتبر التوعية والتدريب جزءًا أساسيًا من استراتيجية إدارة المخاطر. يجب تدريب الموظفين على السياسات والإجراءات الأمنية، وكذلك زيادة وعيهم بالمخاطر المحتملة وكيفية التعامل معها. يمكن تنظيم ورش عمل ودورات تدريبية دورية لتعزيز ثقافة الأمان في الشركة، كما أن التكنولوجيا تلعب دورًا محوريًا في إدارة المخاطر. يمكن استخدام الأنظمة الأمنية المتقدمة مثل أنظمة الكشف عن الاختراق وأنظمة إدارة الهوية والوصول لحماية البيانات والمعلومات الحساسة.

كما يمكن استخدام برامج الذكاء الاصطناعي لتحليل البيانات والكشف المبكر عن التهديدات. والتعاون مع الجهات الخارجية مثل الجهات الحكومية وشركات الأمن الخاصة يمكن أن يكون فعالاً في إدارة المخاطر. يمكن لهذه الجهات تقديم الخبرات والدعم اللازمين لتحسين إجراءات الأمن والحماية، إن أحد الاستراتيجيات الفعالة للتخفيف من المخاطر المالية هو تنويع الاستثمارات والموارد. يساعد هذا التنوع في تقليل تأثير الخسائر المالية المحتملة.

وهذا يحدث عن طريق توزيع المخاطر عبر مجالات مختلفة، ولذلك تعتبر التأمينات أحد الأدوات الفعالة للتخفيف من المخاطر. يمكن للشركات الحصول على تأمينات تغطي مجموعة متنوعة من المخاطر مثل التأمين ضد الكوارث الطبيعية، والتأمين الصحي للموظفين، والتأمين ضد الاختراقات السيبرانية.

يمكن للشركات تحقيق مستوى عالٍ من الأمن والاستقرار من خلال تبني استراتيجيات فعالة لإدارة المخاطر. من خلال التقييم الشامل، والتخطيط الوقائي، واستخدام التكنولوجيا المتقدمة، والتدريب المستمر، يمكن للشركات تحسين قدرتها على مواجهة التحديات وضمان استمرارية أعمالها. تواجه الشركات في المملكة العربية السعودية بيئة أعمال مليئة بالتحديات والفرص على حد سواء. مع التطور السريع في التكنولوجيا وزيادة التهديدات الأمنية، أصبحت إدارة المخاطر جزءاً لا يتجزأ من استراتيجيات الشركات لضمان استمرارية العمل وحمايته من التهديدات المختلفة. يتضمن ذلك التعامل مع المخاطر المالية، التشغيلية، الأمنية، والسيبرانية بشكل منهجي وفعال.

يوجد عدة أخطار لهذه تواجه هذه الشركات منها الأخطار المالية التي تتمثل في عدم الاستقرار الاقتصادي، التغيرات في أسعار الصرف والفوائد، وتقلبات السوق المالية. قد تؤدي هذه المخاطر إلى خسائر مالية كبيرة تؤثر على قدرة الشركة على تحقيق أرباحها واستمراريتها. ومنها المخاطر التشغيلية التي تتعلق بالأخطاء البشرية، الأعطال التكنولوجية، والنقص في الموارد. يمكن لهذه المخاطر أن تؤدي إلى توقف العمليات وتأخير الإنتاج، مما يؤثر على سمعة الشركة وعلاقتها بعملائها.

مشكلة الدراسة:

تحديد المشكلة

تتمثل المشكلة الرئيسية لهذه الدراسة في عدم كفاية الاستراتيجيات الحالية لإدارة المخاطر في العديد من الشركات السعودية. بالرغم من الجهود المبذولة، لا تزال هناك فجوات كبيرة في كيفية التعامل مع المخاطر المختلفة، مما يعرض هذه الشركات لمجموعة متنوعة من التهديدات. تتعدد أسباب هذه الفجوات وتشمل نقص الوعي بالمخاطر، التغيرات السريعة في البيئة التكنولوجية، وكذلك التغيرات المستمرة في القوانين واللوائح التنظيمية.

دراسة المشكلة

من هذه المخاطر التي تهدد أمن الشركات السعودية المخاطر المالية التي تتمثل في التغيرات في أسعار الصرف، تقلبات السوق، والتغيرات في أسعار الفائدة. هذه المخاطر يمكن أن تؤدي إلى تقلبات كبيرة في الإيرادات والأرباح، مما يؤثر بشكل مباشر على الاستقرار المالي للشركة، ويمكن أن تؤدي التغيرات المفاجئة في أسعار النفط إلى تقلبات حادة في الإيرادات للشركات العاملة في قطاع الطاقة. بالإضافة إلى ذلك، يمكن للتغيرات في أسعار الفائدة أن تؤثر على تكلفة التمويل والقروض، مما يزيد من أعباء الديون على الشركات.

من المخاطر التي تهدد الشركات هي المخاطر الأمنية أي هي التهديدات الفيزيائية مثل السرقة والتخريب، وكذلك التهديدات السيبرانية مثل الاختراقات والهجمات الإلكترونية. تتطلب هذه المخاطر استراتيجيات حماية فعالة لضمان سلامة الأصول المادية والبيانات الحساسة، وتعتبر الهجمات السيبرانية من أبرز التهديدات الأمنية التي تواجه الشركات في المملكة. يمكن لهذه الهجمات أن تؤدي إلى سرقة البيانات الحساسة أو تعطيل الأنظمة الحيوية، مما يسبب خسائر مالية كبيرة ويضر بسمعة الشركة.

وتأتي المخاطر السيبرانية الهجمات الإلكترونية، البرمجيات الخبيثة، وسرقة البيانات. في العصر الرقمي، أصبحت هذه المخاطر من أخطر التهديدات التي تواجه الشركات، حيث يمكن أن تؤدي إلى خسائر مالية كبيرة وتضر بسمعة الشركة، وتتضمن الهجمات عبر البرمجيات الخبيثة (مثل الفيروسات وأحصنة طروادة)، وهجمات الفدية التي تطالب بفدية لإعادة الوصول إلى البيانات أو الأنظمة المحتجزة، والهجمات التي تستهدف سرقة البيانات الحساسة من الشركات.

إن فهم المخاطر والتوعية بها يعد جزءاً أساسياً من استراتيجية إدارة المخاطر الفعالة. من دون الوعي الكافي، قد تتخذ الشركات قرارات خاطئة تؤدي إلى زيادة المخاطر بدلاً من التقليل منها، ومن بين الأسباب الرئيسية لنقص الوعي بالمخاطر في الشركات السعودية هو عدم تقديم التدريب الكافي للموظفين، وعدم توفر ثقافة إدارة المخاطر بشكل واسع داخل المنظمة. هذا يمكن أن يؤدي إلى تجاهل المخاطر المحتملة وعدم الاستعداد الجيد للتعامل معها، إن الشركات السعودية تواجه تحدياً كبيراً في مواكبة التغيرات التكنولوجية السريعة. يجب على الشركات تحديث أنظمتها بانتظام للتصدي للتهديدات الجديدة والاستفادة من التكنولوجيا لتحسين كفاءة العمليات وتقليل الأخطاء البشرية.، تتضمن الأمثلة على التغيرات التكنولوجية الهامة التحول نحو الحوسبة السحابية، والتبني المتزايد للتكنولوجيا الذكية والإنترنت، وتطور تقنيات الذكاء الاصطناعي والتعلم الآلي لتحسين تحليل البيانات واتخاذ القرارات.

تشهد المملكة العربية السعودية تغيرات مستمرة في القوانين واللوائح التنظيمية. يتطلب الامتثال لهذه التغيرات تعديل سياسات وإجراءات الشركات بشكل مستمر، مما يمثل تحديًا كبيرًا لإدارة المخاطر، وتتضمن على التغيرات التنظيمية التعديلات في القوانين المتعلقة بحماية البيانات، وزيادة متطلبات الامتثال للمعايير الدولية، وكذلك التغيرات في السياسات الاقتصادية التي تؤثر على العمليات التجارية.

تشير الأدلة إلى أن العديد من الشركات في المملكة لا تزال تعتمد على استراتيجيات إدارة مخاطر تقليدية وغير كافية. تشمل هذه الاستراتيجيات الاعتماد الكبير على التأمين، وضعف استخدام التكنولوجيا المتقدمة، وقلة التدريب والتوعية.

تشمل الثغرات الرئيسية في الاستراتيجيات الحالية نقص التكامل بين أنظمة إدارة المخاطر، الاعتماد المفرط على الإجراءات الورقية، وعدم كفاية الاستجابة السريعة للأزمات. هذا يعرض الشركات لخطر الفشل في مواجهة التهديدات الجديدة والمعقدة، تتضمن الاستراتيجيات المتكاملة لإدارة المخاطر تحليل المخاطر بشكل شامل، وتطوير خطط وقائية واستجابة فعالة، واستخدام التكنولوجيا المتقدمة، وزيادة الوعي والتدريب. هذه الاستراتيجيات تساعد في تحسين كفاءة العمليات وتقليل تأثير المخاطر، ويمكن تطبيق الاستراتيجيات المتكاملة من خلال اعتماد نهج شامل يشمل جميع جوانب إدارة المخاطر. يجب أن تتضمن هذه الاستراتيجيات تحديد المخاطر، تقييمها، وضع خطط وقائية واستجابة، وتنفيذ برامج تدريب وتوعية مستمرة.

أهمية الدراسة:

تعتبر الشركات عموداً فقيراً في الاقتصاد بالنسبة للمملكة العربية السعودية ، والتي تلعب دوراً فعالاً في دعم النمو الاقتصادي وتوفير فرص العمل. تحقيق الأمن الشامل يسهم في استقرار البيئة الأعمال، ويشجع على الاستثمارات المحلية والأجنبية، مما يعزز من الاقتصاد الوطني بشكل عام.

أحد أهم المجالات التي تشملها الاستراتيجيات الفعالة لإدارة المخاطر في مجال أمن الشركات هو تحليل الضعف والفجوات في نظم الأمان الحالية. من خلال هذا التحليل، يمكن للشركات تحديد النقاط الضعيفة واتخاذ التدابير اللازمة لتعزيز الأمان والحد من المخاطر المحتملة. كما يتضمن العمل على وضع سياسات وإجراءات صارمة للأمن، وضمان التزام جميع الموظفين بهذه السياسات كجزء من ثقافة الشركة.

بالإضافة إلى ذلك، فإن التدريب والتوعية يلعبان دوراً مهماً في تعزيز الوعي بالأمان بين الموظفين وتعزيز قدراتهم على التعامل مع التهديدات الأمنية المحتملة بفعالية. علاوة على ذلك، يمكن أن تسهم التكنولوجيا المتقدمة، مثل أنظمة الكشف عن التسلل والحماية من البرمجيات الخبيثة، في تعزيز الأمان الرقمي للشركات والحد من التهديدات السيبرانية.

إن النجاح يتطلب في هذه الجهود التعاون الوثيق مع السلطات الحكومية والمنظمات ذات الصلة لضمان الامتثال للتشريعات الأمنية المحلية والدولية، وتبادل المعلومات والخبرات للتصدي للتهديدات الأمنية على نطاق واسع، إن دراسة استراتيجيات إدارة المخاطر والتخفيف منها في مجال أمن الشركات في المملكة العربية السعودية تعزز من قدرة الشركات على التكيف مع التحديات المتزايدة، وتعزز من سمعتها واستدامتها في السوق المحلي والعالمي.

إن إدارة المخاطر الفعالة والتخفيف منها في مجال أمن الشركات تتطلب تبني نهج شامل يجمع بين التكنولوجيا الحديثة، السياسات الواضحة، التوعية المستمرة، والتعاون مع الخبراء. المملكة العربية السعودية تشهد تحولاً رقمياً كبيراً ، مما يجعل الحاجة إلى استراتيجيات فعالة لإدارة المخاطر أكثر أهمية من أي وقت مضى. تبني هذه الاستراتيجيات، يمكن للشركات في المملكة تعزيز أمانها وحماية أصولها بشكل أفضل.

تتضمن أهمية الدراسة نقاط عدة ومن أهمها :-

- يساهم تحقيق الأمن الشامل في الشركات في زيادة الثقة بين العملاء والشركاء التجاريين، ويحافظ على سمعة الشركة ويقلل من تأثيرات الخسائر المحتملة بسبب الهجمات السيبرانية.
- تعزيز الاستقرار الاقتصادي والنمو المستدام في المملكة العربية السعودية، ويدفع الشركات للالتزام بالمعايير الأمنية الدولية، مما يعزز من قدرتها على المنافسة العالمية.
- يحمي المعلومات الحساسة والبيانات الشخصية للعملاء والموظفين، ويعزز من فرص استقطاب الاستثمارات الأجنبية المهمة للاقتصاد الوطني. بل ويسهم في تحقيق التكامل الرقمي والتحول الرقمي في القطاع الخاص.
- التشجيع على التطوير والابتكار في حلول الأمن التكنولوجي، يقلل من تكاليف استعادة البيانات والأنظمة بعد الهجمات السيبرانية.

- الحد من التبعات القانونية والغرامات المالية بسبب انتهاكات الأمن، و يعزز من استعداد الشركات لمواجهة التحديات الأمنية المستقبلية، كما أنه يساهم في تحقيق الاستدامة البيئية والاجتماعية من خلال الحد من الاستهلاك غير الضروري للموارد.
- يدعم في تطبيق أفضل الممارسات في مجال الأمن السيبراني والفيزيائي، ويزيد من مرونة الشركات في التعامل مع التهديدات المتغيرة. إنه يعزز من مستوى الثقة بين الشركات والجهات الحكومية والمستهلكين.
- الحماية من الاستنزاف الاقتصادي نتيجة للسرقة الإلكترونية والتجسس الصناعي، وتحسين الأداء التشغيلي للشركات بشكل عام.
- المساهمة في تطوير وتعزيز البنية التحتية الرقمية الوطنية. كما أنه يحافظ على استمرارية الأعمال في وجه الكوارث والأزمات الأمنية، وتعزيز الثقافة الأمنية داخل المؤسسات والمجتمع بشكل عام.
- المراقبة المستمرة للأنظمة وتحليل البيانات هو جزء أساسي من إدارة المخاطر. يساعد ذلك في اكتشاف أي نشاط غير عادي في وقت مبكر، مما يتيح للشركة اتخاذ الإجراءات اللازمة قبل تفاقم المشكلة، ولذلك يجب أن يكون لدى الشركات خطة طوارئ واضحة ومحددة للتعامل مع أي حادث أمني. هذه الخطة يجب أن تتضمن خطوات محددة لإدارة الأزمة، وإعادة تشغيل الأنظمة المتأثرة، والتواصل مع الأطراف المعنية.
- مواجهة تقييم أداء استراتيجيات الشركات الأمنية بشكل دوري وإجراء مراجعات دورية للسياسات والإجراءات. هذا يساعد في اكتشاف أي نقاط ضعف وتحسين الاستراتيجيات بشكل مستمر، التعاون مع شركات الأمن السيبراني وخبراء الأمن يمكن أن يوفر رؤى إضافية ويساعد في تعزيز استراتيجيات إدارة المخاطر. الخبراء يمكنهم تقديم استشارات مهنينة وتنفيذ اختبارات الاختراق لتحسين الأنظمة الأمنية.

أهداف الدراسة:

من أهم أهداف تلك الدراسة أنها تقوم بـ

- تحليل التهديدات والضعف: الهدف الرئيسي هو تحليل التهديدات الحالية والمحتملة التي تواجه الشركات في المملكة العربية السعودية، بما في ذلك التهديدات السيبرانية والفيزيائية، وتحديد الضعف في نظم الأمان الحالية.
- تطوير استراتيجيات الأمن: وضع استراتيجيات فعالة تهدف إلى حماية البيانات والمعلومات الحساسة، وتعزيز الأمن الرقمي والفيزيائي للشركات، بما يشمل وضع سياسات صارمة وإجراءات محكمة.
- تعزيز الوعي والتدريب: تعزيز وعي الموظفين بأهمية الأمن والسلامة، وتوفير التدريب المستمر لهم للتعرف على أحدث التقنيات والممارسات في مجال الأمن.
- استخدام التكنولوجيا المتقدمة: تطبيق أحدث التقنيات المتقدمة في مجال الأمن مثل أنظمة الكشف عن التسلل والحماية من البرمجيات الخبيثة، لتعزيز القدرة على اكتشاف واحتواء الهجمات بشكل فعال.
- الامتثال للتشريعات الأمنية: ضمان الامتثال للتشريعات الأمنية المحلية والدولية، وتطبيق المعايير القانونية والتقنية اللازمة لضمان الحماية القانونية والمالية للشركات.
- تعزيز الاستجابة للأزمات: تطوير استراتيجيات فعالة للتعامل مع الأزمات الأمنية والاستجابة السريعة لها، للحد من التأثيرات السلبية وضمان استمرارية الأعمال.

- تحسين الأداء العملياتي: تحسين كفاءة وفعالية العمليات الأمنية داخل الشركات، وتعزيز التكامل بين أقسام الأمن والإدارات الأخرى لتعزيز التعاون والتنسيق.
- تعزيز الثقة العامة: بناء ثقة العملاء والشركاء والمستثمرين بفعالية الأمان والحماية التي توفرها الشركات، مما يساهم في تعزيز سمعتها وزيادة فرص النمو والاستثمار.
- تعزيز الابتكار والتطوير: تشجيع الشركات على الابتكار في حلول الأمن والتكنولوجيا، وتطوير الحلول المبتكرة التي تتكيف مع التهديدات المتغيرة والتطلعات المستقبلية. من خلال تشجيع البحث والتطوير، وتبني التقنيات والحلول الجديدة التي تظهر في السوق.
- تحقيق الاستدامة الاقتصادية: تعزيز الاستدامة الاقتصادية للشركات من خلال الحفاظ على الثروات والموارد وتقليل التكاليف الناجمة عن الاستجابة لحوادث الأمن، ولذلك فإنها تهدف إلى تحقيق أمان شامل واستقرار اقتصادي، وتعزيز قدرة الشركات على التكيف مع التحديات المتزايدة والمحافظة على استدامتها في السوق المحلي والعالمي.
- تحديد المخاطر الأمنية المحتملة: إن هذه الدراسة تسعى إلى تحديد وفهم مجموعة المخاطر الأمنية المحتملة التي تواجه الشركات في المملكة. تشمل هذه المخاطر الهجمات السيبرانية، سرقة البيانات، الاختراقات، والتجسس الصناعي، ومنه إلى تحليل الوضع الحالي لإدارة أمن المعلومات في الشركات السعودية. يتضمن ذلك تقييم السياسات والإجراءات الحالية، البنية التحتية التقنية، والوعي الأمني بين الموظفين.

- تطوير إطار عمل متكامل : وهذا من خلال تطوير إطار عمل متكامل لإدارة المخاطر الأمنية يناسب البيئة السعودية. يشمل هذا الإطار السياسات والإجراءات، الحلول التقنية، وخطط الاستجابة للطوارئ.
- تعزيز التعاون بين القطاعين العام والخاصة : تتجه الدراسة نحو تعزيز التعاون بين القطاعين العام والخاص في مجال أمن المعلومات. يتضمن ذلك توصيات لتبادل المعلومات، تنظيم ورش عمل ومؤتمرات، وتطوير شراكات استراتيجية، وأيضاً تعزيز قدرة الشركات على التكيف مع التهديدات الأمنية المتغيرة والمتطورة. يشمل ذلك تطوير استراتيجيات مرنة وقابلة للتعديل بشكل مستمر.
- تحديد أفضل الممارسات العالمية : من خلال استعراض أفضل الممارسات العالمية في مجال إدارة المخاطر الأمنية. يشمل ذلك تحليل استراتيجيات الشركات الرائدة دولياً والتوصيات الصادرة عن الهيئات والمنظمات المعنية بأمن المعلومات، كما يتم تقييم الاستثمارات الحالية في مجال الأمن وتقديم توصيات حول كيفية تحسينها. يشمل ذلك تحليل التكلفة والفائدة لبرامج وأدوات الحماية المختلفة.

تساؤلات الدراسة

من خلال مناقشة أهمية وأهداف هذه الدراسة ، أقوم بطرح عدة أسئلة تفسر هذه النظرية

ومنها:-

أولاً : الأسئلة الرئيسية

- ما هي التهديدات الرئيسية التي تواجه الشركات في مجال الأمن في السعودية؟ وكيف يؤثر التهديد السيبراني على أمن الشركات في المملكة العربية السعودية؟
- ما هي أبرز استراتيجيات إدارة المخاطر التي تستخدمها الشركات في المملكة العربية السعودية ، وما هو دور التدريب والتوعية في تعزيز الأمن داخل الشركات؟

ثانيا: الأسئلة الفرعية

- ما هي التقنيات المتقدمة التي يمكن استخدامها لتعزيز الأمن السيبراني في الشركات؟
- كيف يؤثر الامتثال للتشريعات الأمنية على استراتيجيات الشركات في السعودية؟
- ما هي أهمية بناء ثقة العملاء والشركاء في استراتيجيات إدارة المخاطر؟
- كيف يمكن للشركات تحقيق التوازن بين الأمن والابتكار في بيئة الأعمال؟ وما هي التحديات الرئيسية التي تواجه الشركات في تنفيذ استراتيجيات الأمن؟ وكيف يمكن للشركات تقييم فعالية استراتيجيات إدارة المخاطر التي تنفذها؟
- ما هو تأثير انتهاكات البيانات على الشركات وكيف يمكن التصدي لهذه الانتهاكات؟ وكيف يمكن للشركات تحديد مستوى التهديدات والمخاطر المحتملة لأمنها؟

فروض الدراسة:

توضح هذه الفروض أهمية الدراسة في استكشاف وتحليل التحديات وتطوير الحلول لتحقيق أمن شامل واستقرار اقتصادي في السعودية، وتشتمل على :-

- تحديد التهديدات الرئيسية: من خلال الفرضيات، يتم التركيز على تحليل وتحديد التهديدات الأمنية الرئيسية التي تواجه الشركات في المملكة العربية السعودية، مثل الهجمات السيبرانية والتجسس الصناعي والتهديدات الفيزيائية. حيث تواجه الشركات في المملكة العربية السعودية مستوى متزايداً من التهديدات السيبرانية نتيجة للتحول الرقمي السريع والاعتماد المتزايد على التكنولوجيا، وتبحث الدراسة في مدى تأثير التحول الرقمي على زيادة التهديدات السيبرانية، بما في ذلك الهجمات الخبيثة وسرقة البيانات.

- تقييم الضعف والفجوات: دراسة مفصلة للضعف والفجوات في أنظمة الأمان الحالية للشركات، وذلك لتحديد المناطق التي تحتاج إلى تعزيز وتحسين لضمان الحماية الشاملة.
- تطوير استراتيجيات مبتكرة: تقديم فرضيات حول تطوير استراتيجيات مبتكرة لإدارة المخاطر والتخفيف منها، مثل تكامل التقنيات الحديثة وتعزيز التدابير الأمنية لتعزيز استجابة الشركات للتهديدات.
- أهمية التدريب والتوعية: يتعين أن يتضمن الفرض المؤهلات التي توضح أهمية التدريب المستمر للموظفين والتوعية بمخاطر الأمن، مما يساهم في تعزيز الثقافة الأمنية داخل الشركات.
- المعايير الأمنية: يتم تفصيل فروض حول أهمية الامتثال للمعايير الأمنية المحلية والدولية كجزء من استراتيجيات الأمن الشاملة للشركات.
- التأثير على الاستدامة والنمو الاقتصادي: يتضمن الفرض فحص التأثير الذي تخلفه استراتيجيات إدارة المخاطر على استدامة الأعمال والنمو الاقتصادي في المملكة العربية السعودية.
- الحاجة للتقييم المستمر: حيث التقييم المستمر لاستراتيجيات الأمن السيبراني يساعد في تحسينها وتكييفها مع التهديدات المتغيرة، وهذا يعرض من خلال أهمية التقييم المستمر وتقديم آليات فعالة لتنفيذه.
- الابتكار والتطوير: تسليط الضوء على دور الابتكار والتطوير في تطوير حلول جديدة وفعالة لإدارة المخاطر وتعزيز الأمن في الشركات.
- تحقيق التوازن بين الأمن والأداء العملياتي: تقديم دراسة حول كيفية تحقيق التوازن بين تعزيز الأمان وضمان استمرارية الأعمال وتحسين الأداء العملياتي للشركات.

- تقييم أثر الاستراتيجيات: يشمل الفرض تقييماً لأثر الاستراتيجيات المقترحة على كفاءة وفعالية إدارة المخاطر وتحقيق الأهداف المحددة للأمن في الشركات.
- نقص في الوعي الأمني بين موظفي الشركات السعودية، مما يزيد من مخاطر الاختراقات الأمنية، وتقوم الدراسة بتقييم مستوى الوعي الأمني بين الموظفين ومدى تأثير هذا النقص على الأمان العام للشركات.
- تأثير التكنولوجيا المتقدمة: استخدام التكنولوجيا المتقدمة مثل الذكاء الاصطناعي والتحليل الكبير للبيانات يمكن أن يحسن بشكل كبير من إدارة المخاطر الأمنية، تناقش الدراسة كيفية تطبيق التكنولوجيا المتقدمة في تحسين أمن المعلومات وتخفيف المخاطر.
- أهمية التدريب المستمر: التدريب المستمر والتوعية الأمنية يمكن أن يقلل بشكل كبير من المخاطر الأمنية في الشركات السعودية، من خلالها يتم التأثير على برامج التدريب المستمر على الوعي الأمني وفعالية استراتيجيات إدارة المخاطر.
- التعاون بين القطاعين العام والخاص: وهذا يمكن أن يعزز من فعالية استراتيجيات إدارة المخاطر الأمنية، ويناقش هذا من خلال نماذج التعاون الناجحة وتقترح آليات لتعزيز هذا التعاون في المملكة.
- أثر الجائحة على الأمن السيبراني: جائحة كوفيد-19 أدت إلى تغييرات في بيئة العمل تسببت في زيادة التهديدات الأمنية للشركات. حيث تأثير الجائحة على الأمن السيبراني وكيفية الشركات مع هذه التحديات الجديدة.

- **التفاوت بين القطاعات:** هناك تفاوت في مستوى الأمن السيبراني بين مختلف القطاعات الاقتصادية في المملكة، يعالج ذلك بتحليل هذا التفاوت وتقديم توصيات لتحسين الأمن في القطاعات الأقل حماية.
- **نقص الموارد المالية:** نقص الموارد المالية المخصصة للأمن السيبراني في بعض الشركات يعوق تنفيذ استراتيجيات فعالة لإدارة المخاطر، وستبحث الدراسة في تأثير الميزانيات المحدودة على الأمن السيبراني وتقترح طرقاً لتخصيص الموارد بشكل أكثر فعالية.
- **أثر الثقافة التنظيمية:** توجد داخل الشركات وتؤثر على فعالية تنفيذ استراتيجيات الأمن السيبراني، حيث تحليل الثقافة التنظيمية وكيفية تحسينها لدعم استراتيجيات الأمن السيبراني.

الدراسات السابقة:

- العتيبي ، خالد ، 2021، تحديات الأمن السيبراني في الشركات السعودية: استراتيجيات وحلول، ط1، المملكة العربية السعودية، المجلة السعودية للإدارة.
- القحطاني ، سارة ، 2021، استراتيجيات الأمن السيبراني للشركات السعودية: دراسة ميدانية، ط1، المملكة العربية السعودية، دار المجلة السعودية للأبحاث العلمية.
- العتيبي، هالة، 2021، الأمن السيبراني وإدارة المخاطر في المؤسسات التعليمية السعودية ، جامعة الملك فيصل بالمملكة العربية السعودية، دار الجامعة للنشر.
- النفيعي، محمد. 2021، استراتيجيات التخفيف من المخاطر في النقل، ط1، الرياض، دار المسيرة.
- الغامدي، عبدالله، 2020، إدارة المخاطر في الشركات: أفضل الممارسات في السعودية، ط1، المملكة العربية السعودية، مجلة الإدارة العامة.

- آل خليفة، خالد، 2020، الأمن السيبراني في الشركات الحكومية والخاصة في دول مجلس التعاون الخليجة، ط1، جامعة البحرين- مجلس التعاون الخليجي،
- السعدي، أحمد، 2020، تحديات الأمن السيبراني في الشركات الصغيرة والمتوسطة في الشرق الأوسط، ط2، جامعة الإمارات.
- القحطاني، صالح، 2020، استراتيجيات إدارة المخاطر في قطاع النفط والغاز في المملكة العربية السعودية، ط2، جامعة البترول والمعادن .
- العبدلي، خالد، 2020، إدارة الأزمات في الشركات السعودية، المملكة العربية السعودية، ط4، مكتبة الأمل بالدمام.
- القحطاني، مروان ، 2019، تقييم فعالية سياسات الأمن السيبراني في الشركات السعودية، ط2، المملكة العربية السعودية، المجلة العربية للأمن السيبراني.
- الزهراني، علي، 2019، تحليل المخاطر السيبرانية وتأثيرها على الشركات في السعودية، ط2، المملكة العربية السعودية، دار المجلة العربية للأمن السيبراني.
- السبيعي، نواف، 2019، استراتيجيات التخفيف من المخاطر في التعليم، ط1، الرياض ،دار الهداية.
- الدوسري، مريم، 2019، أمن المعلومات وإدارة المخاطر في الشركات السعودية، ط1، المملكة العربية السعودية، دارالجامعة للنشر.
- السليمان، فهد، 2019، التحول الرقمي وأثره على الأمن السيبراني في المملكة العربية السعودية، ط1، المملكة العربية السعودية، جامعة الملك عبد العزيز.
- المانع، عبدالله، 2019، تحليل مخاطر الأمن السيبراني في القطاع المالي السعودي، ط1، المملكة العربية السعودية، معهد الإدارة العامة.
- العتيبي، ماجد، 2018، تقييم سياسات الأمن في الشركات السعودية: دراسة حالة، ط3، المملكة العربية السعودية، دار المجلة العلمية.

- الزبيدي، حسن. 2018، إدارة المخاطر في القطاع الصناعي، ط2، جدة، دار العلوم.
- المطيري، ناصر. 2018، إدارة المخاطر في القطاع الصحي، ط2، المدينة المنورة، دار الأفق.
- الحربي، ناصر، 2018، التدريب والتوعية الأمنية في الشركات العربية: حالة دراسية في المملكة العربية السعودية، ط1، جامعة الإمام محمد بن سعود الإسلامية.
- العتيبي، خالد، 2018، تأثير التكنولوجيا الحديثة على أمن المعلومات في الشركات الخليجية، ط1، جامعة الكويت.
- الصالح، محمد، 2018، استراتيجيات إدارة المخاطر في الشركات السعودية: دراسة تحليلية، ط2، المملكة العربية السعودية، دار المنظومة للنشر والتوزيع.
- الشمري، فاطمة، 2017، إدارة المخاطر في الشركات السعودية: نماذج وتطبيقات، ط1، المملكة العربية السعودية، بمجلة الإدارة العامة.
- الشداددي، علي، 2017، إدارة المخاطر الأمنية في الشركات العربية، المملكة العربية السعودية، ط1، جامعة الملك سعود.
- عبد الله، حامد، 2017، استراتيجيات الوقاية من المخاطر في التعليم، ط3، الطائف، دار الفاروق.
- الشمري، عبدالرحمن، 2016، إدارة المخاطر وأمن المعلومات في الشركات السعودية، المملكة العربية السعودية، ط1، دار الثقافة للنشر والتوزيع.

المنطلقات النظرية للدراسة:

تعد إدارة المخاطر والتخفيف منها من الجوانب الحيوية في أمن الشركات، حيث أن الشركات في المملكة العربية السعودية تواجه مجموعة متنوعة من المخاطر التي تتطلب استراتيجيات فعالة لإدارتها والتخفيف من تأثيرها. إن البيئة الاقتصادية والسياسية المتغيرة، والتقدم التكنولوجي، وتزايد التهديدات الأمنية، تجعل من الضروري تبني نهج شامل لإدارة المخاطر.

إنها عملية تحديد وتقييم والتحكم في المخاطر المحتملة التي قد تؤثر على أهداف المنظمة. تشمل هذه المخاطر المالية، والتشغيلية، والاستراتيجية، والامتثال، والأمنية. الهدف الأساسي هو حماية الأصول، والحفاظ على الاستمرارية التشغيلية، وتحقيق الأهداف الاستراتيجية.

استراتيجيات إدارة المخاطر:

- الابتعاد عن الأنشطة أو العمليات التي تنطوي على مخاطر عالية.
- اتخاذ إجراءات لتقليل احتمالية حدوث المخاطر أو تقليل تأثيرها.
- نقل المخاطر إلى طرف ثالث من خلال التأمين أو العقود.
- قبول المخاطر التي تكون تكلفتها منخفضة أو تأثيرها غير كبير.

وهذا من خلال: تطوير خطة إدارة المخاطر: تحديد الإجراءات المحددة للتعامل مع كل مخاطرة. توزيع الموارد: تخصيص الموارد اللازمة لتنفيذ استراتيجيات التخفيف. مراقبة البيئة الداخلية والخارجية لاكتشاف التغيرات التي قد تؤثر على المخاطر. إعادة تقييم المخاطر واستراتيجيات التخفيف بانتظام.

الاستراتيجيات الفعالة لإدارة المخاطر في مجال أمن الشركات:

- تطوير خطط أمنية شاملة تغطي جميع جوانب العمليات.
- تعزيز الأمن السيبراني من خلال استخدام تقنيات حديثة ونظم حماية قوية.
- تدريب الموظفين بانتظام على أفضل الممارسات الأمنية ورفع مستوى الوعي حول المخاطر الأمنية.
- التعاون مع الجهات الحكومية والأمنية لتعزيز الأمن الشامل.
- إجراء تقييمات دورية للإجراءات الأمنية وتطويرها وفقاً لأحدث التهديدات.

التحديات الخاصة في المملكة العربية السعودية:

تواجه الشركات في السعودية تحديات فريدة مثل التهديدات السيبرانية المستمرة، والاحتياجات الأمنية الخاصة بالبنية التحتية الحرجة، والامتثال للمتطلبات التنظيمية الصارمة. تعد القدرة على التكيف مع التغيرات السريعة في البيئة الأمنية أمراً بالغ الأهمية لضمان استمرارية الأعمال. تتطلب إدارة المخاطر والتخفيف منها في مجال أمن الشركات نهجاً متكاملاً يجمع بين التحليل الدقيق للمخاطر، وتطوير استراتيجيات شاملة، وتنفيذها بفعالية. إن الاستثمار في التكنولوجيا، وتدريب الموظفين، وتعزيز التعاون مع الجهات الخارجية، تعتبر من العوامل الرئيسية لنجاح استراتيجيات إدارة المخاطر في المملكة العربية السعودية.

نظرية إدارة المخاطر: تعد نظرية إدارة المخاطر واحدة من الركائز الأساسية في هذه الدراسة. تهدف هذه النظرية إلى التعرف على المخاطر المحتملة التي يمكن أن تواجه الشركات، وتقييم تأثيرها، وتطوير استراتيجيات للحد منها أو إدارتها بشكل فعال. تشمل هذه النظرية عدة خطوات رئيسية:

- تحديد المخاطر: التعرف على جميع التهديدات المحتملة سواء كانت داخلية أو خارجية.
- تحليل المخاطر: تقييم احتمالية حدوث المخاطر وتأثيرها على الشركة.
- تقييم المخاطر: تحديد الأهمية النسبية لكل خطر بناءً على احتمالية حدوثه وتأثيره.
- إدارة المخاطر: تطوير وتنفيذ استراتيجيات للحد من تأثير المخاطر أو التخفيف منها.

نظرية الأمن السيبراني: في عصر التحول الرقمي، أصبحت نظرية الأمن السيبراني محورية في حماية البيانات والمعلومات الحساسة للشركات. تعتمد هذه النظرية على حماية الأنظمة والشبكات من الهجمات الإلكترونية من خلال:

- التشفير: حماية البيانات من الوصول غير المصرح به.
- الجدران النارية: منع الوصول غير المصرح به إلى الشبكات.
- التدقيق الأمني: مراجعة الأنظمة بانتظام للكشف عن الثغرات الأمنية.
- الاستجابة للحوادث: تطوير خطط استجابة فعالة للتعامل مع الهجمات السيبرانية.

نظرية الإدارة الاستراتيجية: تعتبر الإدارة الاستراتيجية جزءاً لا يتجزأ من إدارة المخاطر. تعتمد هذه النظرية على تطوير رؤية ورسالة واضحة للشركة، وتحليل البيئة الداخلية والخارجية لتحديد نقاط القوة والضعف، والفرص والتهديدات. تساعد هذه النظرية ، وأنها خطة مخصصة توضح بالتفصيل كيفية تعامل المؤسسات مع المخاطر المختلفة، سواء بشكل استباقي أو عند وقوع الحوادث، وبذلك توفر نظرة تفصيلية لرواد الأعمال والمديرين التنفيذيين حتى يتمكنوا من اتخاذ قرارات مستنيرة،

وتعد استراتيجية إدارة المخاطر جزءًا أساسيًا لأي خطة في هذا الخصوص، ومن ثم يتم تحديد هذه الاستراتيجية بعد تحديد المخاطر وتقييم احتمالية حدوثها، بالإضافة إلى التأثير الذي يمكن أن تحدثه، ومن ثم سوف يحتاج واضع الاستراتيجية إلى تحديد كيفية التعامل والنهج الذي سيتبعه لإدارة المخاطر وعلاجها، وتتمثل في :

- تحليل البيئة: فهم العوامل الاقتصادية والاجتماعية والتكنولوجية والقانونية التي تؤثر على الشركة.
- تطوير الاستراتيجيات: وضع استراتيجيات فعالة تستند إلى تحليل البيئة لضمان تحقيق الأهداف التنظيمية.
- التنفيذ والمتابعة: تنفيذ الاستراتيجيات ومراقبة الأداء لضمان تحقيق النتائج المرجوة.

نظرية المرونة التنظيمية: تركز هذه النظرية على قدرة الشركات على التكيف مع التغيرات غير المتوقعة والتعامل مع الأزمات بفعالية. تساعد المرونة التنظيمية في:

- التكيف السريع: تعديل العمليات والاستراتيجيات بسرعة لمواجهة التهديدات الجديدة.
- التعلم التنظيمي: الاستفادة من التجارب السابقة لتحسين الاستعداد للأزمات المستقبلية.
- التعاون الداخلي: تعزيز التعاون بين الإدارات المختلفة لتحقيق استجابة منسقة للأزمات.

نظرية التغيير التنظيمي : توضح هذه النظرية كيفية تنفيذ التغييرات الضرورية في الهياكل والعمليات التنظيمية لضمان الأمان والاستدامة. تُشمل هذه النظرية:

- التخطيط للتغيير: وضع خطط تفصيلية للتغيير تتضمن الأهداف والاستراتيجيات والإجراءات.
- إدارة التغيير: التعامل مع مقاومة التغيير من خلال التواصل الفعال وإشراك جميع أصحاب المصلحة.
- تنفيذ التغيير: تنفيذ الخطط بفعالية لضمان تحقيق الأهداف المرجوة:

نظرية التحليل الكمي والنوعي للمخاطر: يستخدم التحليل الكمي أدوات رياضية وإحصائية لتقييم المخاطر بناءً على البيانات التاريخية والمعطيات الحالية، بينما يعتمد التحليل النوعي على الخبرات والتقديرات الشخصية. كلا النوعين من التحليل يعتبران مهمين في:

- تقدير الاحتمالات: استخدام النماذج الرياضية لتقدير احتمالية وقوع المخاطر.
- تقييم التأثير: تحليل الآثار المحتملة للمخاطر على العمليات التنظيمية.
- تطوير الاستراتيجيات: استخدام نتائج التحليل لتطوير استراتيجيات فعالة لإدارة المخاطر.

نظرية حوكمة الشركات: تركز هذه النظرية على مبادئ الشفافية والمساءلة والعدالة في إدارة الشركات. تُسهم الحوكمة الجيدة :

- تعزيز الثقة: بناء الثقة بين المستثمرين وأصحاب المصلحة من خلال ضمان النزاهة والشفافية.
- الحد من المخاطر: وضع سياسات وإجراءات قوية للحد من المخاطر المحتملة.

- تحسين الأداء: تحسين الأداء التنظيمي من خلال توفير بيئة عمل آمنة ومستقرة.

نظرية العلاقات الدولية: تعتبر العلاقات الدولية جزءاً من البيئة الخارجية التي تؤثر على الشركات. تسهم هذه النظرية :

- فهم التأثيرات الخارجية: فهم التأثيرات الجيوسياسية والاقتصادية على الشركات.

- التكيف مع السياسات: التكيف مع السياسات والتشريعات الدولية التي تؤثر على الأمن وإدارة المخاطر.

- تعزيز التعاون: تعزيز التعاون الدولي لتبادل الخبرات وأفضل الممارسات في إدارة المخاطر.

نظرية التنافسية العالمية: تركز هذه النظرية على كيفية تحقيق الشركات للميزة التنافسية في السوق العالمي من خلال الابتكار والأمان. تسهم هذه النظرية :

- تحليل السوق: فهم اتجاهات السوق العالمية وتحديد الفرص والتهديدات.

- تعزيز الابتكار: تعزيز الابتكار في المنتجات والخدمات لتحسين التنافسية.

- تحقيق الميزة التنافسية: استخدام استراتيجيات الأمان لإدارة المخاطر وتعزيز الميزة التنافسية.

- تساعد الدراسة في تقديم إطار شامل لتحليل وتطوير استراتيجيات فعالة لإدارة المخاطر في الشركات السعودية. تسهم هذه النظريات في تقديم فهم أعمق للمخاطر والتحديات التي تواجه الشركات وتوفير الحلول المبتكرة للتغلب عليها وضمان الأمن والاستدامة في بيئة الأعمال الديناميكية.

المنهجية وطرق البحث:

- هذه الدراسة بها نوعين من الطرق : النوعي والكمي ، حيث سيتم جمع البيانات من خلال المقابلات والاستبيانات وتحليل البيانات الإحصائية.
- استخدام النهج المختلط ، حيث سيتم الجمع بين البيانات الكمية والنوعية
- إجراء مقابلات متعمقة مع خبراء الأمن، مديري المخاطر، والمستشارين في الشركات السعودية للحصول على رؤى حول الاستراتيجيات الحالية والتحديات.
- توزيع استبيانات على عدد كبير من الشركات لجمع بيانات كمية حول ممارسات إدارة المخاطر وأداء الأمن.
- مراجعة الأدبيات الأكاديمية والمقالات والدراسات السابقة المتعلقة بإدارة المخاطر والأمن السيبراني.
- تحليل التقارير الصادرة عن الجهات الحكومية والمؤسسات الخاصة حول المخاطر والأمن في الشركات السعودية.
- استخدام قواعد البيانات الأكاديمية مثل Google Scholar ، JSTOR ، PubMed للحصول على دراسات ومقالات ذات صلة.
- سيتم تحليل البيانات الكمية من خلال استخدام البرامج الإحصائية مثل SPSS أو Excel لتحليل البيانات الكمية المجمعة من الاستبيانات. وسيتم استخدام الإحصاءات الوصفية (مثل المتوسطات والانحرافات المعيارية) والإحصاءات الاستدلالية (مثل التحليل التبايني والانحدار) لفحص العلاقات بين المتغيرات المختلفة.
- تحليل البيانات النوعية: تحليل البيانات النوعية المجمعة من المقابلات باستخدام تقنيات التحليل الموضوعي (Thematic Analysis) لتحديد الأنماط والموضوعات الرئيسية المتعلقة بإدارة المخاطر والأمن.

إطار العمل الزمني:

المرحلة التحضيرية:لتصميم أدوات البحث والحصول على الموافقات اللازمة.

جمع البيانات:.....لجمع البيانات من المصادر الأولية والثانوية.

تحليل البيانات:..... لتحليل البيانات الكمية والنوعية.

كتابة التقرير : لإعداد التقرير النهائي وتقديم النتائج والتوصيات.

أدوات الدراسة :

تحديد العينة: اختيار عينة ممثلة من الخبراء والمديرين بناءً على معايير محددة مثل الخبرة والموقع الجغرافي.

إعداد دليل المقابلة: تطوير قائمة بالأسئلة المفتوحة والمركزة على محاور الدراسة مثل التحديات والفرص في إدارة المخاطر.

إجراء المقابلات: تنظيم مقابلات فردية وجماعية، إما وجهاً لوجه أو عبر الإنترنت، وتسجيل الإجابات بموافقة المشاركين.

تحليل البيانات: تحليل الإجابات باستخدام التحليل الموضوعي لتحديد الأنماط والأفكار الرئيسية.

تصميم الاستبيان: تطوير استبيان يحتوي على أسئلة مغلقة ومفتوحة تغطي محاور الدراسة مثل استراتيجيات إدارة المخاطر والتدابير الأمنية، وهذا من خلال:

اختبار تجريبي: إجراء اختبار تجريبي للاستبيان على عينة صغيرة لتحسين الأسئلة وضمان وضوحها.

توزيع الاستبيان: إرسال الاستبيانات إلى الشركات عبر البريد الإلكتروني أو من خلال الزيارات الميدانية.

جمع البيانات: تجميع الاستبيانات المعبأة وتحليلها باستخدام البرامج الإحصائية.

جمع الوثائق: جمع وتحليل الأدبيات الأكاديمية، التقارير الرسمية، والأبحاث السابقة المتعلقة بإدارة المخاطر والأمن السيبراني.

تحليل الوثائق: استخدام تحليل المحتوى لاستخلاص المعلومات الرئيسية والأنماط ذات الصلة بالدراسة.

تحديد المواقع: اختيار شركات محددة بناءً على تنوع الأنشطة والمخاطر التي تواجهها.

تسجيل الملاحظات: مراقبة الإجراءات الأمنية وتسجيل الملاحظات بشكل منظم.

تحليل الملاحظات: تحليل الملاحظات لاستخلاص النقاط القوية والضعيفة في الممارسات الأمنية.

التحليل الإحصائي:

إعداد البيانات: ترميز وتنظيم البيانات في جداول إحصائية.

استخدام البرامج الإحصائية: استخدام برامج مثل SPSS أو Excel لإجراء التحليلات الإحصائية الوصفية والاستدلالية.

تفسير النتائج: تفسير النتائج الإحصائية لاستخلاص الاستنتاجات والتوصيات.

حدود الدراسة :

أولاً : الحدود الموضوعية

تركز الدراسة على استراتيجيات إدارة المخاطر والتخفيف منها في مجال أمن الشركات. تشمل الموضوعات الرئيسية التي سيتم تناولها:

تحليل المخاطر: التعرف على أنواع المخاطر التي تواجهها الشركات وكيفية تحليلها وتقييمها.

استراتيجيات إدارة المخاطر: استراتيجيات فعالة لتقليل المخاطر والسيطرة عليها.

الأمن السيبراني: الإجراءات والتدابير المتبعة لحماية البيانات والمعلومات من الهجمات السيبرانية.

التدريب والتوعية: دور التدريب والتوعية في تحسين إدارة المخاطر.

التكنولوجيا: استخدام التكنولوجيا المتقدمة في تحسين الأمن وإدارة المخاطر.

الاستثناءات: لا تشمل الدراسة الشركات التي لا تواجه مخاطر أمنية عالية أو تلك التي تعمل في قطاعات غير متعلقة بالأمن السيبراني بشكل مباشر.

ثانيا : الحدود المكانية

تشمل الدراسة على الشركات والمؤسسات التي تعمل في المملكة العربية السعودية، اختيار عينة متنوعة من الشركات تشمل مختلف القطاعات (مثل التكنولوجيا، المالية، الصناعة، والخدمات).

تغطي الدراسة المناطق الرئيسية في المملكة مثل الرياض، جدة، الدمام، ومكة المكرمة لضمان تنوع الجغرافيا وتغطية الشركات في مختلف البيئات الاقتصادية.

ثالثا: الحدود الزمانية

تمتد فترة جمع البيانات والتحليل على مدى شهر، من 9/6/2024 إلى 10/7/2024، وستراعي الدراسة التغيرات الموسمية والاقتصادية التي قد تؤثر على إدارة المخاطر والأمن السيبراني في الشركات.

المراجع:

- الغامدي، عبدالله، 2020، إدارة المخاطر في الشركات: أفضل الممارسات في السعودية، مجلة الإدارة العامة للنشر، ط1، ص: 56-85.
- القحطاني، مروان، 2019، تقييم فعالية سياسات الأمن السيبراني في الشركات السعودية، المجلة العربية للأمن السيبراني للنشر والتوزيع، ط2، ص: 141.
- الزهراني، علي، 2019، تحليل المخاطر السيبرانية وتأثيرها على الشركات في السعودية، دار المجلة العربية، ط2، ص: 96-102.
- الدوسري، مريم، 2019، أمن المعلومات وإدارة المخاطر في الشركات السعودية، دار الجامعة للنشر، ط1، ص: 36-40.
- العتيبي، ماجد، 2018، تقييم سياسات الأمن في الشركات السعودية: دراسة حالة، دار المجلة العلمية، ط3، ص: 58.
- الصالح، محمد، 2018، استراتيجيات إدارة المخاطر في الشركات السعودية: دراسة تحليلية، دار المنظومة للنشر والتوزيع، ط2، ص: 106.
- الشمري، فاطمة، 2017، إدارة المخاطر في الشركات السعودية: نماذج وتطبيقات، مجلة الإدارة العامة، ط1، ص: 60-67.
- الشمري، عبد الرحمن، 2016، إدارة المخاطر وأمن المعلومات في الشركات السعودية، دار الثقافة للنشر والتوزيع، ط1، ص: 85-93.
- العتيبي، خالد، 2021، تحديات الأمن السيبراني في الشركات السعودية: استراتيجيات وحلول، المجلة السعودية للإدارة، ط1، ص: 108.
- القحطاني، سارة، 2021، استراتيجيات الأمن السيبراني للشركات السعودية: دراسة ميدانية، دار المجلة السعودية للأبحاث العلمية، ط1، ص: 204-219.
- العبدلي، خالد، 2020، إدارة الأزمات في الشركات، مكتبة الأمل بالدمام، ط4، ص: 85.

- الحربي، راشد، 2019، إدارة المخاطر التشغيلية في المؤسسات، دار المنارة بالرياض، ط1، ص: 131-139.
- الشدادى، علي، 2017، إدارة المخاطر الأمنية في الشركات العربية، جامعة الملك سعود، مناقشة التحديات التي تواجه الشركات العربية في مجال إدارة المخاطر الأمنية، واقتراح حلول لها، ص: 117-123.
- العمري، سالم، 2021، إدارة المخاطر المالية، دار الأندلس بجدة، ط2، ص: 116.
- المطيري، ناصر. 2018، إدارة المخاطر في القطاع الصحي، دار الأفق بالمدينة المنورة، ط2، ص: 115-123.
- العتيبي، خالد، 2018، تأثير التكنولوجيا الحديثة على أمن المعلومات في الشركات الخليجية، جامعة الكويت، كيف يمكن للتكنولوجيا الحديثة أن تعزز أمن المعلومات في الشركات الخليجية، ص: 97.
- الجهني، فهد، 2017، إدارة المخاطر البيئية، دار الفكر للطائف، ط1، ص: 49-55.
- العتيبي، محمد. 2016، إدارة المخاطر في المشاريع الصغيرة، دار الشروق بالرياض، ط3، ص: 142.
- السليمان، فهد، 2019، التحول الرقمي وأثره على الأمن السيبراني في المملكة العربية السعودية، جامعة الملك عبد العزيز، تأثير التحول الرقمي السريع في المملكة، ص: 204-210.
- السبيعي، نواف، 2019، استراتيجيات التخفيف من المخاطر في التعليم، دار الهداية بالرياض، ط1، ص: 50-62.
- الزبيدي، حسن. 2018، إدارة المخاطر في القطاع الصناعي، دار العلوم، جدة، ط2، ص: 145-158.
- النفيعي، محمد. 2021، استراتيجيات التخفيف من المخاطر في النقل، دار المسيرة، الرياض، ط1، ص: 86-91.
- الراشد، يوسف، 2017، المخاطر في البنوك، دار اليازوري، الرياض، ط4، ص: 204.

- البقمي، خالد. 2019، إدارة المخاطر في قطاع العقارات، دار الأفق، جدة، ط2، ص:49-58.
- العمرو، عبد الله، 2020، إدارة المخاطر في الشركات الناشئة، دار التقدم، مكة المكرمة، ط2، ص: 110-129
- الحسن، علي، 2015، إدارة المخاطر التشغيلية في المصانع دار الفاروق، جدة، ط2، ص:77-82.
- المانع، عبدالله، 2019، تحليل مخاطر الأمن السيبراني في القطاع المالي السعودي، معهد الإدارة العامة، ط1، ص: 94.
- السعد، محمد. 2020، إدارة المخاطر في المشاريع الإنشائية، دار النشر العربي، الرياض. ط2، ص:91.
- الرافعي، سالم، 2017، استراتيجيات التخفيف من المخاطر في الصناعة، دار الفكر، مكة المكرمة. ط3، ص:84-91.
- العتيبي، هالة، الأمن السيبراني وإدارة المخاطر في المؤسسات التعليمية السعودية، 2021، بجامعة الملك فيصل، البحث في التحديات الأمنية التي تواجه المؤسسات التعليمية في المملكة، ص: 87-91.
- عبد العزيز، محمد، 2016، استراتيجيات الوقاية من المخاطر في الزراعة، دار المسيرة، الطائف. ط1، ص: 60-85.
- عبد الله، حسان، 2018، إدارة المخاطر في المشاريع الإنشائية، دار الفكر، جدة. ط2، ص:112-126.
- علي، محمد، 2020، إدارة المخاطر التشغيلية في النقل، دار النور، الرياض. ط3، ص:72-78.
- عبد الله، حامد، 2017، استراتيجيات الوقاية من المخاطر في التعليم، دار الفاروق، الطائف، ط3، ص:55، 57

- عبد العظيم، طاهر، 2019، إدارة المخاطر في الشركات، دار الفكر، الرياض، ط4، ص:90.
- <https://www.arrajol.com/content/324706/%D8%A5%D8%AF%D8%A7%D8%B1%D8%A9-%D9%88%D8%A3%D8%B9%D9%85%D8%A7%D9%84/%D8%A5%D8%AF%D8%A7%D8%B1%D8%A9-%D8%A7%D9%84%D9%85%D8%AE%D8%A7%D8%B7%D8%B1-%D8%A7%EF%BB%B7%D9%85%D9%86%D9%8A%D8%A9-rakan-aljouid>
- <https://ae.linkedin.com/pulse/%D8%A5%D8%AF%D8%A7%D8%B1%D8%A9-%D8%A7%D9%84%D9%85%D8%AE%D8%A7%D8%B7%D8%B1-%D8%A7%EF%BB%B7%D9%85%D9%86%D9%8A%D8%A9-rakan-aljouid>
- <https://www.ncsc.gov.bh/ar/cyberwiser/professionals/network-enterprise/cyber-risks-for-leaders.html>