

عنوان البحث

أثر تبني استراتيجيات الأمن السيبراني على استدامة المشاريع التقنية الناشئة في المملكة العربية السعودية

إعداد الطالب/ ياسر حسن الصفدي

الرقم الجامعي/ 243000055

إشراف الدكتور / أحمد راجح

العام الدراسي:

2025

قائمة المحتويات:

2	قائمة المحتويات:
3	مقدمة:
5	مشكلة الدراسة:
6	أهمية الدراسة:
7	اهداف الدراسة:
8	تساؤلات الدراسة:
9	فرضيات الدراسة:
9	الدراسات السابقة:
16	المنطلقات النظرية للدراسة:
18	المنهجية وطرق البحث:
20	أدوات الدراسة:
21	حدود الدراسة:
23	المراجع:

المقدمة:

في ظل الثورة الرقمية العالمية المتسارعة، أصبحت مبادرات التكنولوجيا الجديدة عناصر أساسية في إرساء اقتصاد المعرفة وتشجيع الابتكار، لا سيما في الدول التي تسعى إلى الريادة التقنية، مثل المملكة العربية السعودية. ويتمشى هذا التوجه مع رؤية المملكة 2030، التي تهدف إلى تنويع مصادر الدخل وتشجيع الاستثمار في التكنولوجيا وريادة الأعمال. ومع تزايد الاعتماد على الأنظمة الرقمية، برزت مخاطر الأمن السيبراني كواحدة من أبرز الصعوبات التي تواجه تطوير المبادرات، لا سيما في مراحلها الأولى، التي تتسم بالحساسية ونقص البنية التحتية الأمنية.

لم يعد اعتماد أساليب قوية للأمن السيبراني خياراً؛ بل أصبح ضرورة لضمان استمرارية هذه المبادرات واستمراريتها على المدى الطويل في عالم رقمي يتميز بالتغيرات السريعة والمخاطر العديدة. يمكن أن تتسبب الهجمات الإلكترونية وتسريب البيانات والاختراقات في انقطاع العمليات وفقدان الثقة، بل وحتى فشل المشروع في مراحله الأولى. ونتيجة لذلك، يُعد تحقيق التوازن بين الابتكار التقني والحماية الأمنية أمراً بالغ الأهمية لتطوير مبادرات تكنولوجيا قادرة على التوسع والمنافسة. وبناءً على ذلك، تُعد هذه الدراسة بالغة الأهمية، إذ ستبحث في تأثير تطبيق أساليب الأمن السيبراني على استدامة مبادرات تطوير التكنولوجيا في المملكة. وتركز على فهم العقبات التي تواجهها هذه المبادرات، ومدى إدراك رواد الأعمال لضرورة الأمن السيبراني، والتقنيات المستخدمة لتطبيقه بفعالية. ويهدف البحث من خلال ذلك إلى تقديم نصائح عملية تُساعد هذه المبادرات على أن تصبح أكثر مرونة وتزدهر في بيئة رقمية آمنة ومستدامة.

يُحدث التنبؤ العالمي للتقنيات الجديدة تحولاتٍ في الاقتصادات والثقافات والصناعات بوتيرةٍ غير مسبوقة، مُبشراً بعصرٍ ثوريٍّ تحوّل فيه الابتكار من ميزةٍ تنافسيةٍ إلى ضرورةٍ مُلحةٍ. تُغيّر تقنيات الذكاء الاصطناعي، والروبوتات، وإنترنت الأشياء، والبلوك تشين (blockchain) طريقة عمل الشركات وتعاونها لإنتاج القيمة. هذه الثورة عالمية النطاق، وتؤثر على كلّ من الدول المتقدمة والنامية. يستثمر كلّ من القطاعين العام والتجاري استثماراتٍ كبيرةً في الحلول الرقمية لزيادة الكفاءة، ودفع عجلة التنمية الاقتصادية، ومعالجة التحديات المجتمعية الصعبة.

في السنوات الأخيرة، ساد اعتقادٌ متزايدٌ بأن تطوير التقنيات قد يجعل الخدمات أكثر مرونةً وسلاسةً وقابليةً للتوسع عبر مجموعةٍ واسعةٍ من الصناعات، بما في ذلك الرعاية الصحية والتعليم والتمويل والتصنيع. وقد أتاحت هذه التقنيات فرصاً

جديدةً لجمع البيانات وتحليلها وأتمتة المهام وتطوير تجارب مُصمّمة خصيصًا. وفي نهاية المطاف، يؤدي هذا إلى زيادة الإنتاجية وتحسين عملية اتخاذ القرارات. تُدرك الدول في جميع أنحاء العالم الأهمية الاستراتيجية لتبني هذه التقنيات، التي تُوفّر مزايا اقتصاديةً مع معالجة مخاوف رئيسيةٍ مثل تغيّر المناخ، والوصول إلى الرعاية الصحية، واستدامة البنية التحتية. ومع ذلك، فإن طريق تبني التقنيات الناشئة محفوف بالعقبات، لا سيما فيما يتعلق بحماية البيانات، والأمن السيبراني، وتشريد العمال، والفجوة الرقمية، وتعقيدات التنفيذ. لذا، فإن اتباع استراتيجية متوازنة تُعطي الأولوية للابتكار أمرٌ بالغ الأهمية للحكومات التي تسعى إلى تحقيق كامل إمكانات التقنيات الجديدة (dga, 2025).

نفذت المملكة العربية السعودية مجموعة متنوعة من المبادرات كجزء من استراتيجيتها للذكاء الاصطناعي، بما في ذلك:

- **تميز المواهب:** تهدف جهود تميز المواهب إلى تطوير كفاءة المملكة المستقبلية في مجال الذكاء الاصطناعي. وتهدف إلى جعل المملكة مركزًا عالميًا للتدريب والتعليم في مجال الذكاء الاصطناعي من خلال التعاون مع الأكاديميين والجمهور وقطاع الأعمال.
- **المؤسسات الرائدة في مجال الذكاء الاصطناعي:** يشرف المركز الوطني للذكاء الاصطناعي (NCAI) على المهام والمبادرات المتعلقة بالذكاء الاصطناعي في العديد من القطاعات. كما يشرف على مبادرات تطبيق تقنيات الذكاء الاصطناعي، ويقدم الدعم لمنظومة الصناعة، ويضمن تحقيق الأهداف الوطنية.
- **البحث والتطوير:** يُجري المركز الوطني للذكاء الاصطناعي (NCAI) أبحاثًا أساسية وتطبيقية في مجال الذكاء الاصطناعي، مما يجعله المركز الوطني للابتكار في هذا المجال. ويشجع المركز على ترجمة نتائج الأبحاث إلى تطبيقات وحلول عملية، مما يعزز الاقتصاد القائم على المعرفة.
- **مراكز الابتكار:** يعزز مركز الابتكار التابع للمركز الوطني للذكاء الاصطناعي الابتكار وريادة الأعمال من خلال تسهيل إنشاء تطبيقات وحلول الذكاء الاصطناعي. يتعاون المركز مع الشركات الناشئة وحاضنات الأعمال لسد الفجوة بين التعليم والتوظيف، مما يتيح للشركات الجديدة المساهمة في التنمية الاقتصادية للمملكة.

- المبادرات: تسعى مبادرة "واحة الذكاء الاصطناعي" إلى تعزيز المعرفة العامة بالذكاء الاصطناعي من خلال عروض تفاعلية وفعاليات تعليمية. تدمج هذه المبادرة التكنولوجيا مع تاريخ وثقافة المملكة العربية السعودية الغنيين، مما يخلق تجربة تفاعلية تشجع الشباب على البحث عن وظائف في مجال البيانات والذكاء الاصطناعي.
- القمة العالمية: تُعد القمة العالمية للذكاء الاصطناعي، التي تنظمها الهيئة السعودية للبيانات والذكاء الاصطناعي، منصة رئيسية للحوار الدولي حول الذكاء الاصطناعي. عُقد الحدث الافتتاحي رقميًا يومي 21 و22 أكتوبر 2020، وجمع سياسيين وباحثين ومستثمرين ورواد أعمال وخبراء تكنولوجيا لتحديد مستقبل الذكاء الاصطناعي (my, 2025).

مشكلة الدراسة:

مع التقدم المستمر في التكنولوجيا الرقمية، أصبحت مبادرات التكنولوجيا الجديدة في المملكة العربية السعودية ركيزة أساسية في النظام الاقتصادي الحديث، معتمدةً بشكل أساسي على الحلول الرقمية والبيانات المصاحبة لها. ومع ذلك، ونظرًا لاعتمادها المتزايد على البيئة الرقمية، أصبحت هذه المبادرات أكثر عرضة للهجمات السيبرانية، مما قد يؤثر بشكل مباشر على استمراريتهما واستمراريتهما. على الرغم من مساعي الحكومة لتحسين الأمن السيبراني على المستوى الوطني، لا تزال العديد من المبادرات النامية تفتقر إلى سياسات أمنية محددة، أو لا تُعطي الأمن السيبراني الأولوية في خططها التشغيلية، إما بسبب نقص المعرفة أو الموارد. وهذا يجعلها أكثر عرضة لتهديدات مثل القرصنة، واختراق البيانات، والأعطال التكنولوجية.

ومن هنا، تتجلى مشكلة الدراسة في السؤال التالي:

- إلى أي مدى يُسهم تطبيق أساليب الأمن السيبراني في تحسين استدامة مبادرات التكنولوجيا النامية في المملكة العربية السعودية؟

تنبع هذه المشكلة من عدد من الأسئلة الفرعية، منها:

- ما مدى وعي رواد الأعمال العاملين في مبادرات التكنولوجيا الجديدة بمخاطر الأمن السيبراني؟
- ما هي استراتيجيات الأمن الأكثر استخدامًا في هذه المشاريع؟
- هل هناك علاقة بين نشر تقنيات الأمن السيبراني واستدامة المشاريع أو نموها؟ ما هي عقبات تطبيق هذه الاستراتيجيات في بيئة الشركات الناشئة؟

أهمية الدراسة:

تكتسب هذه الدراسة أهميتها من كونها تجمع بين اتجاهين حاليين مهمين: الأمن السيبراني والمبادرات التكنولوجية الناشئة. وكلاهما ركيزتان أساسيتان في التحول الرقمي للمملكة العربية السعودية واستدامة أعمالها على المدى الطويل. ونظرًا للتوجه الوطني لرؤية السعودية 2030 نحو اقتصاد قائم على المعرفة والابتكار، ثمة حاجة ملحة لفهم دور الأمن السيبراني كعامل تمكين لاستمرار هذه المبادرات وتوسيع نطاقها.

أولاً: الأهمية العلمية

- زيادة الفهم النظري للعلاقة بين أساليب الأمن السيبراني وجدوى المشاريع الناشئة، لا سيما في ظل العالم الرقمي الحالي.
- تناول الدراسة نقصًا في البحث العلمي في الأدبيات العلمية العربية من خلال دراسة العلاقة بين الأمن السيبراني واستدامة المشاريع الجديدة، والتي كانت محدودة.
- تؤسس هذه الورقة البحثية أساسًا علميًا للبحوث المستقبلية في مجال التقاء التكنولوجيا وريادة الأعمال وإدارة المخاطر.

ثانيًا: الأهمية العملية

- يُثَقِّفُ البحث رواد الأعمال ومديري مشاريع التكنولوجيا الجديدة حول ضرورة دمج أساليب الأمن السيبراني في عملياتهم اليومية وتخطيطهم الاستراتيجي.
- ويُقَدِّمُ مؤشرات وإجراءاتٍ فعّالةٍ لاعتماد وتنفيذ سياسات أمن سيبراني فعّالةٍ للحفاظ على الاستمرارية وتقليل المخاطر.
- ويُثَقِّفُ الجهات الحكومية وجهات دعم الشركات الناشئة حول ضرورة تقديم المشورة والمساعدة في مجال الأمن السيبراني، مما يضمن استمرارية القطاع على المدى الطويل.
- ويُساعد البحث على تعزيز الفهم المؤسسي والاجتماعي لضرورة الأمن السيبراني كعنصرٍ أساسي في نجاح المشاريع الريادية، وليس مجرد عاملٍ تقنيٍّ ثانوي.

اهداف الدراسة:

الهدف الرئيسي للدراسة:

- تقييم أثر تبني استراتيجيات الأمن السيبراني على استمرارية مشاريع التكنولوجيا الناشئة على المدى الطويل في المملكة العربية السعودية، ومدى مساهمة هذه الاستراتيجيات في الحد من المخاطر، وضمان استمراريّتها، وتعزيز الثقة الرقمية في منظومة ريادة الأعمال.

الأهداف الفرعية للدراسة:

- تحديد مستوى معرفة رواد الأعمال في مبادرات التكنولوجيا الجديدة بأهمية الأمن السيبراني ومخاطره.
- رصد مختلف تقنيات الأمن السيبراني المستخدمة في مبادرات التكنولوجيا الناشئة، ومدى شموليتها وفعاليتها.

- دراسة العلاقة بين تطبيق أساليب الأمن السيبراني ومقاييس استدامة المشاريع، مثل النمو، والاحتفاظ بالعملاء، واستمرارية العمليات.
- دراسة أبرز القضايا الملحة التي تواجه مشاريع التكنولوجيا الجديدة في وضع تدابير فعالة للأمن السيبراني.
- تقديم توصيات واقعية لتحسين كفاءة وفعالية الأمن السيبراني في منظومة ريادة الأعمال التكنولوجية، مما يزيد من فرص نجاح المشاريع واستمراريتها على المدى الطويل.

تساؤلات الدراسة:

التساؤل الرئيسي:

- ما تأثير أساليب الأمن السيبراني على استمرارية الشركات التقنية الناشئة في المملكة العربية السعودية على المدى الطويل؟

التساؤلات الفرعية:

- إلى أي مدى يدرك رواد الأعمال في الشركات التقنية الناشئة مخاطر الأمن السيبراني؟
- ما هي أكثر أساليب الأمن السيبراني شيوعاً التي تستخدمها الشركات التقنية الناشئة؟
- ما العلاقة بين تطبيق سياسات الأمن السيبراني وتحقيق أهداف الاستدامة، مثل استمرارية الشركة ونموها؟
- ما هي العقبات التي يواجهها رواد الأعمال في مجال التكنولوجيا في المملكة في وضع استراتيجيات فعالة للأمن السيبراني؟
- كيف يمكن تطبيق أساليب الأمن السيبراني بشكل أفضل لمساعدة شركات التكنولوجيا على الازدهار؟

فرضيات الدراسة:

الفرضية الرئيسية:

- يوجد أثر ذو دلالة إحصائية لتبني استراتيجيات الأمن السيبراني على استدامة المشاريع التقنية الناشئة في المملكة العربية السعودية.

الفرضيات الفرعية:

- يرتبط فهم رواد الأعمال لمخاوف الأمن السيبراني ارتباطاً إيجابياً بطول عمر شركات التكنولوجيا.
- سياسات الأمن السيبراني الشاملة والناجحة لها تأثير إيجابي على استمرارية شركات التكنولوجيا على المدى الطويل.
- يمكن أن يساعد تطبيق أساليب الأمن السيبراني الشركات على التخفيف من التحديات التكنولوجية وتحقيق نجاح طويل الأمد.
- تُصعّب تحديات البنية التحتية والمالية والخبرة التقنية اعتماد حلول فعالة للأمن السيبراني.
- يُحسن توافر الدعم المؤسسي والإشراف الحكومي من نجاح أساليب الأمن السيبراني بين شركات التكنولوجيا.

الدراسات السابقة:

يُسلّط بحث (dga, 2025) التحليلي لاستراتيجيات التحوّل الرقمي في المملكة العربية السعودية الضوء على الدور المحوري لهيئة الحكومة الرقمية في مساعدة مختلف المؤسسات الحكومية على تحقيق أهدافها في التحوّل الرقمي وتطبيق حلول مبتكرة. وفي هذا الصدد، تُقدّم الهيئة مجموعة متنوعة من الخدمات الاستشارية، مثل تحليل مبادرات التحوّل الرقمي والتأكد من توافقها مع الأهداف الوطنية للتحوّل الرقمي. وقد شكّلت هذه الخدمات أساساً لبحثنا. في عالم يشهد تحوّلًا رقميًا متسارعًا، تطمح المملكة العربية السعودية إلى أن تكون في طليعة هذه الثورة. وفي هذا السياق، يُقدّم تقرير البحث الصادر عن هيئة الحكومة

الرقمية لمحة عامة عن أنشطة المؤسسات الحكومية في هذا الصدد، مُستعرضًا مجالات التحسين المهمة والأهداف الاستراتيجية والجوانب المشتركة عبر برامج التحول الرقمي. ويُقدّم هذا التقرير نظرة شاملة على رحلة التحول الرقمي في المملكة وتوصيات للخطوات التالية.

برزت بيانات الاختبار التنظيمية كأداة مهمة لتسريع تبني التقنيات الجديدة في المملكة العربية السعودية. فهي توفر بيئة خاضعة للرقابة، تُمكن الشركات الناشئة والشركات الصغيرة والمتوسطة والشركات القائمة من اختبار الحلول والسلع والخدمات الرقمية المبتكرة تحت إشراف الجهات التنظيمية المختصة. تدعم هذه البرامج أهداف رؤية 2030 من خلال تعزيز النمو الاقتصادي، وتحفيز الاستثمار، وتسهيل تطوير صناعات تكنولوجية جديدة. أنشأت العديد من الجهات الحكومية بيئات اختبارية لمعالجة قطاعات وتطبيقات تكنولوجية محددة:

- أنشأ البنك المركزي السعودي بيئة اختبارية تنظيمية تُركز على التكنولوجيا المالية. يُشجع هذا البرنامج الشركات المحلية والأجنبية المهتمة بتطوير خدمات مالية رقمية مبتكرة في بيئة ديناميكية وخاضعة للرقابة. يهدف البرنامج إلى تحسين المعرفة بتأثير هذه التقنيات على القطاع المالي في المملكة، ومساعدتها على التطور لتصبح مركزًا ماليًا ذكيًا.
- تسعى بيئة اختبار تطبيقات التوصيل إلى تنظيم ومراقبة قطاعي البريد وتطبيقات التوصيل. يُعزز هذا المشروع توسيع منظومة التوصيل من خلال تقصير وقت التسويق، وخفض تكاليف الخدمة، والسماح لمطوري التطبيقات باختبار خدمات جديدة. إنها تفيد جميع المعنيين، بما في ذلك العملاء والمنتجين ومقدمي خدمات التوصيل.
- يهدف صندوق الاختبار التنظيمي للتقنيات الناشئة إلى مساعدة الشركات على اختبار الحلول المبتكرة القائمة على التقنيات المتقدمة مثل إنترنت الأشياء (IoT)، والبلوك تشين، والحوسبة السحابية، والذكاء الاصطناعي (AI)، والواقع المعزز والافتراضي (AR)، والتوائم الرقمية، والطباعة ثلاثية/رباعية الأبعاد. تتيح صناديق الاختبار هذه للشركات الناشئة والقائمة اختبار نماذج وخدمات الأعمال المبتكرة ضمن إطار تنظيمي مرن. كما يستفيد المشاركون من انخفاض عدم اليقين التنظيمي، وعمليات الموافقة السريعة، وسهولة الوصول إلى التمويل.
- كما طورت هيئة الحكومة الرقمية برنامج صندوق اختبار حصريًا لشركات التكنولوجيا الحكومية. ويسعى إلى التحقيق في المنصات والخدمات الرقمية الجديدة في القطاع العام والإشراف عليها، وتحسين البيئة التنظيمية

لخدمات الحكومة الرقمية، وتحسين تجربة المستخدم من خلال حل المشكلات التنظيمية التي تواجهها الشركات والمنظمات في هذا المجال(my, 2025).

في عام ٢٠٢٤، أحرزت المملكة العربية السعودية تقدماً ملحوظاً في تعزيز بيئة ريادة الأعمال والابتكار، في إطار جهودها المتواصلة لتحقيق رؤية ٢٠٣٠، التي تهدف إلى تنويع الاقتصاد الوطني. وتولي المملكة اهتماماً بالغاً بدعم الشركات الناشئة، باعتبارها عنصراً أساسياً في توفير فرص عمل جديدة ودفع عجلة النمو الاقتصادي طويل الأجل. تواصل المملكة تعزيز بيئة ديناميكية من خلال عدد من البرامج الحكومية ومشاريع الدعم التي تستهدف تسريع نمو الشركات الناشئة في قطاعات متنوعة، بما في ذلك التكنولوجيا، والطاقة المتجددة، والرعاية الصحية، والتعليم، وغيرها. وفي ظل هذه البيئة، طورت العديد من الجهات الحكومية والشركات مبادرات تمويلية، بالإضافة إلى منصات استثمارية، لمساعدة الشركات على الحصول على التمويل اللازم (إبراهيم، 2024).

في إطار هدفها الطموح لرؤية 2030، تبني المملكة العربية السعودية التجديد والابتكار الشاملين لتحقيق تحول اقتصادي واجتماعي سريع. ويوجه الرؤساء التنفيذيون السعوديون شركاتهم للوفاء بالتزامات المملكة القوية ببناء اقتصاد مستدام وجاهز للمستقبل، والتي تشمل تعزيز القطاع الخاص، وإنشاء صناعات وقطاعات جديدة، وتوفير آلاف فرص العمل، وتشجيع المشاريع الخضراء. ويؤدي الرؤساء التنفيذيون السعوديون تفاؤلاً خاصاً بشأن آفاق تنمية الاقتصاد المحلي، حيث توقع 77% منهم نمواً في المملكة خلال الاثني عشر شهراً المقبلة، متجاوزين بذلك نظرائهم الإقليميين والعالميين. وتُعد المملكة الوجهة الاستثمارية الأولى للرؤساء التنفيذيين الإقليميين الآخرين خارج بلدانهم. وفيما يتعلق بالاستدامة، قام 72% من الرؤساء التنفيذيين السعوديين باستثمارات صديقة للمناخ في العام السابق، أي أكثر من نظرائهم في الدول الست التي شملتها الدراسة، مما يشير إلى التزام استباقي بموازنة النمو مع المسؤولية البيئية. ولدى الرؤساء التنفيذيين في المملكة جدول أعمال حافل للعام المقبل، حيث يستكشفون إمكانات السوق الهائلة والتهديدات التي تواجهها، ويعيدون ابتكار شركاتهم للمستقبل (pwc, 2025).

يتناول هذا البحث كيفية مساهمة تكنولوجيا المعلومات في تحقيق أهداف الاستدامة في المملكة العربية السعودية. لا يزال تمكين الشركات من استخدام تكنولوجيا المعلومات بنجاح في مشاريع الاستدامة يمثل صعوبة، لا سيما في المملكة. نقوم

بتحليل أربع دراسات حالة لمعرفة كيف تستخدم الشركات السعودية التكنولوجيا لتحقيق أهداف الاستدامة الخاصة بها. تُظهر النتائج توجهاً كبيراً نحو الجهود الخضراء في المملكة، مع استخدام تقنيات مثل إنترنت الأشياء (IoT) وسلسلة الكتل (blockchain) والذكاء الاصطناعي (AI). لعبت هذه التقنيات دوراً حاسماً في زيادة كفاءة الطاقة وتقليل النفايات. يؤكد البحث على دور التدخلات السياسية والشراكات بين القطاعين العام والخاص في تحقيق الاستدامة البيئية والازدهار الاقتصادي. لتعزيز تطوير الممارسات المستدامة، يجب على الحكومة التركيز على تطوير المهارات الرقمية داخل الشركات وإزالة العقبات التكنولوجية. تُظهر دراسات الحالة لأربع شركات في المملكة العربية السعودية ممارسات مستدامة ومساعدة تكنولوجية مناسبة. تؤكد الدراسة على ضرورة استخدام تكنولوجيا المعلومات والتعاون لتسريع التقدم نحو أهداف الاستدامة الوطنية (Madkhali, 2023).

يهدف هذا المشروع إلى دراسة العوائق والمخاوف المرتبطة بتطبيق ممارسات الأمن السيبراني في المدن الذكية السعودية، بالإضافة إلى تصميم نموذج النظرية الموحدة لقبول واستخدام التكنولوجيا 3 (UTAUT3) القائم على الأمن السيبراني والتحقق منه. وللدراسة هدفان. أولاً، سلطت الضوء على أهم المشاكل والقضايا في تطبيق سياسات الأمن السيبراني في المدن الذكية السعودية. ثانياً، أنشأت نموذجاً قائماً على التكنولوجيا لتطبيق مبادئ الأمن السيبراني في المدن الذكية السعودية. وقد أُجري مسحان لتحقيق هذين الهدفين. كشفت الدراسة الأولية عن مشاكل وثغرات في تطبيق ممارسات الأمن السيبراني في المدن الذكية، بما في ذلك المخاوف بشأن ضعف منصات الأمن السيبراني، وقضايا الخصوصية، وتأثير البنية التحتية الحديثة لتكنولوجيا المعلومات على الثقافة السعودية (ن = 554 من عامة الناس). أما المسح الثاني (ن = 108: متخصصو تكنولوجيا المعلومات) فقد ركز على تطوير نموذج UTAUT3 القائم على الأمن السيبراني والتحقق من صحته، والذي تضمن تسعة عوامل: الأداء المتوقع، والجهد المتوقع، والتأثير الاجتماعي، والظروف التمكينية، والسلامة، والمرونة، والتوافر، والسرية، وسلامة الأمن السيبراني. تم تقييم صحة النموذج وموثوقيته، مما يدل على قدرته على فهم سلوك المستخدم واتجاهات تبني التكنولوجيا في المدن الذكية. وسلطت نتائج الدراسة الضوء على العوامل المؤثرة في تبني تدابير الأمن السيبراني في المدن الذكية السعودية، مؤكدةً على أهمية الاستراتيجيات المحددة، وبرامج التوعية الفعالة، وتعاون الجهات المعنية في تعزيز بيئة رقمية آمنة ومرنة (Alhalafi, 2023).

تتوسع قضايا الأمن السيبراني في الصناعات الخدمية والصناعية في المملكة العربية السعودية مع نمو الاستخدام الرقمي، مما يؤكد على أهمية التدابير الأمنية القوية والوعي بين الشركات الصغيرة والمتوسطة. ونتيجة لذلك، تُعد هذه الدراسة جديدة بالملاحظة نظرًا للاعتماد المتزايد على التكنولوجيا الرقمية ومخاوف الأمن السيبراني الخاصة التي تواجهها الشركات الصغيرة والمتوسطة في هذه القطاعات الاقتصادية الحيوية. مع التقدم التقني السريع، أصبحت قدرات تكنولوجيا المعلومات والأمن السيبراني بالغ الأهمية، لا سيما في بيئة ما بعد كوفيد-19. وقد شهد كل من الصناعات الخدمية والصناعية في المملكة العربية السعودية تحولات كبيرة نحو العمليات الرقمية. وكان الغرض من هذه الدراسة هو التحقيق في تأثير لوائح الأمن السيبراني التنظيمية على المرونة التنظيمية والأداء التجاري طويل الأجل في قطاعي الخدمات والتصنيع في المملكة العربية السعودية، بالإضافة إلى النظر في الآثار الوسيطة والمعتدلة للمرونة التنظيمية والثقافة. وقد تم استخدام استراتيجية دراسة كمية تجمع بين تحليل شامل للأدبيات والبيانات الفعلية من عينة من 394 مشاركًا سعوديًّا، مقسمة بالتساوي بين قطاعي الخدمات والصناعة. وتم استخدام Smart PLS 3.3.3 للتحقق من صحة الفرضيات المقدمة. كشفت النتائج عن تأثير إيجابي لسياسات الأمن السيبراني التنظيمية على مرونة المؤسسة. وكان لقوانين الأمن السيبراني التنظيمية تأثير كبير على أداء الأعمال على المدى الطويل؛ ولم يكن للمرونة والثقافة التنظيمية دورٌ مُخفف. تُعد هذه الدراسة من أوائل الدراسات التي تُقدم مراجعةً منهجيَّةً لقدرات تكنولوجيا المعلومات والأمن السيبراني في قطاعي الخدمات والتصنيع في المملكة العربية السعودية، وخاصةً في فترة ما بعد جائحة كوفيد-19. تُسهم هذه النتائج في النقاش الأكاديمي، ولها آثار إدارية مهمة على الشركات السعودية التي تخوض غمار العصر الرقمي (Al-Somali, 2024).

تهدف دراسة (Al-Zahrani, 2025) إلى استكشاف عوامل النجاح التي دفعت المملكة العربية السعودية إلى صدارة أبحاث الأمن السيبراني. وتسعى إلى توفير إطار شامل للأمن السيبراني يشجع على تبادل المعلومات على مستوى العالم ويعزز معايير الأمن. وتستخدم الدراسة منهجية دراسة الحالة ومنهج البحث النوعي. وقد تناولت الدراسة الأوراق والندشورات المتعلقة بالأمن السيبراني في المملكة العربية السعودية منذ عام 2017، عندما تأسست الهيئة الوطنية للأمن السيبراني، وحتى تصنيفها كأفضل دولة في مؤشر الأمن السيبراني العالمي 2024. وأجري تحليل موضوعي للمواد المدروسة باستخدام معايير PRISMA لاكتشاف الاتجاهات. وتُظهر نتائج الدراسة أن المملكة العربية السعودية قد تفوقت في مجال الأمن السيبراني بفضل عدد من العوامل المهمة، بما في ذلك نموذج حوكمة مركزي يعمل من خلال عمليات لامركزية، واستثمارات كبيرة في الأمن السيبراني، والتعاون

الدولي، وبرنامج تنمية رأس المال البشري الذي يراعي التنوع بين الجنسين. كما تُسلط الدراسة الضوء على ضرورة ربط خطط الأمن السيبراني بالأهداف الوطنية، بالإضافة إلى تعزيز الشراكات بين القطاعين العام والخاص، من أجل تحسين القدرة على مواجهة التهديدات السيبرانية. تُسلط نتائج الدراسة الضوء على عوامل نجاح مهمة ساهمت في ترسيخ مكانة المملكة العربية السعودية كرائدة عالمية في مجال الأمن السيبراني. وتُسلط هذه الدراسة الضوء على عوامل النجاح المهمة التي دفعت المملكة العربية السعودية إلى صدارة تصنيفات الأمن السيبراني. ويمكن أن يُشكّل الإطار المُقترح نموذجًا يُحتذى به للدول الأخرى التي تسعى إلى تحسين قدراتها في مجال الأمن السيبراني، مُسلّطًا الضوء على أهمية اتباع أساليب متكاملة تشمل الحوكمة والاستثمار والتعاون وتنمية الموارد البشرية.

أحدثت الصناعة 5.0 تحولاً في التكنولوجيا من خلال دمج الأنظمة المادية والشبكات الرقمية. وقد أدت هذه التطورات أيضاً إلى زيادة في الهجمات الإلكترونية، مما يشكل مخاطر كبيرة، لا سيما على الشركات الصغيرة والمتوسطة. تبحث هذه الدراسة في مقاومة الشركات الصغيرة والمتوسطة في المملكة العربية السعودية والمملكة المتحدة لتدابير الأمن السيبراني في سياق الصناعة 5.0، مع التركيز على الحوكمة والسياسات. كما تبحث في الأسباب الثقافية والاقتصادية التي تساهم في هذه المقاومة، مثل ضعف فهم مخاوف الأمن السيبراني، والقيود على الميزانية، وتضارب أهداف الشركات. كما يتناول التقرير أهمية السياسات والقوانين الحكومية في تعزيز ممارسات الأمن السيبراني بين الشركات الصغيرة والمتوسطة، بمقارنة أساليب المملكة العربية السعودية مع أساليب المملكة المتحدة. تعتمد الدراسة نهجاً متعدد الأساليب، يشمل مقابلات مع أصحاب الشركات الصغيرة والمتوسطة وخبراء، لتسليط الضوء على الصعوبات وإمكانات تعزيز حوكمة الأمن السيبراني واللوائح التنظيمية في كلا البلدين. وتسلط النتائج الضوء على أهمية الحلول الشخصية، نظراً للاختلافات الثقافية والاقتصادية بين المملكة العربية السعودية والمملكة المتحدة. تُركز الدراسة على معرفة وتطبيق الأمن السيبراني بين الشركات الصغيرة والمتوسطة السعودية، ومدى التزامها بالمبادئ التوجيهية الأساسية لضوابط الأمن السيبراني (ECC-1:2018). كما تتناول أساليب التوعية والامتثال للأمن السيبراني الحالية في المملكة المتحدة، مُقارنةً مواد المشورة الرسمية المُصممة لمساعدة الشركات الصغيرة والمتوسطة على تحسين عملياتها المتعلقة بالأمن السيبراني. ووفقاً لهذه الدراسة، يُقترح زيادة التفاعل مع هذه الأوراق في كلا البلدين لزيادة فهم الشركات الصغيرة والمتوسطة وثقتها وامتثالها، مما يُعزز وضعها الأمني السيبراني. تُقدم هذه الورقة دراسة مُقارنة للحوكمة والسياسات في المملكة العربية السعودية والمملكة المتحدة، مع توصيات لتحسين الوعي والتثقيف في مجال الأمن السيبراني،

وتعزيز الأطر التنظيمية، وتشجيع الشراكات بين القطاعين العام والخاص لمكافحة تهديدات الأمن السيبراني في سياق الثورة الصناعية الخامسة (Rawindaran, 2023).

حققت المملكة العربية السعودية تقدماً هائلاً في مجال الأمن السيبراني. فقد حافظت على إجراءات تنظيمية صارمة للكشف عن المخالفين وتبعهم ومعاقبتهم، مما يحمي مصالح المستخدمين الأفراد والشركات من المخاطر السيبرانية مثل سرقة البيانات. ويؤدي الاعتماد المتزايد على تكنولوجيا المعلومات والخدمات المدعومة بتكنولوجيا المعلومات (ITES) إلى تحسين التدابير الأمنية. وتُعد بيئة التهديد المتغيرة باستمرار للأمن السيبراني قضية مثيرة للجدل. في هذا السياق، تقدم هذه المقالة مراجعة شاملة لكيفية تطور الجرائم الإلكترونية في المملكة العربية السعودية حاليًا، بالإضافة إلى دراسة لبعض أبرز الاعتداءات الإقليمية. وتهدف الأطر والإجراءات التنظيمية الحالية في المملكة العربية السعودية إلى تثبيط السلوك الإجرامي على الإنترنت. وقد تم وضع العديد من نماذج الكفاءة لمعالجة المهارات اللازمة لمنع الجرائم الإلكترونية في هذه البيئة. ويمكن للباحثين في هذا المجال أيضًا الاستفادة من تحديد مستوى الكفاءة الأساسية لضمان الأمن الأمثل. للإجابة على هذه المسألة البحثية، يستخدم هذا التقييم مختبر تجربة وتقييم صنع القرار الضبابي (Fuzzy-DMTAE)، وعملية التسلسل الهرمي التحليلي الضبابي (F.AHP)، ومنهج TOPSIS الضبابي لتحسين كفاءة سياسات الأمن السيبراني القطاعية. يتناول هذا التقييم أوجه التشابه والاختلاف بين هذه المناهج الثلاثة. ويحدد هذا التقييم للأمن السيبراني أن المركز الوطني للأمن السيبراني (NCSC) يُمثل أولوية قصوى. ويواصل التقرير تحليل الصعوبات التي يجب دراستها ومعالجتها من أجل بناء إجراءات أمن سيبراني أكثر مصداقية وفعالية، مما يؤدي إلى اقتصاد قائم على خدمات تكنولوجيا المعلومات (ITES) أكثر تمكينًا في المملكة العربية السعودية. علاوة على ذلك، يجب على خبراء الأمن السيبراني والمسؤولين العمل معًا للدفاع عن الأصول الرقمية للبلاد في عصر الحرب السيبرانية العلنية والسرية (Alhakami, 2024).

باعتباره أحد أهداف التنمية المستدامة، يُعدّ "التعليم للجميع" أمرًا بالغ الأهمية. ومع ذلك، فقد جلب الانخراط في قطاع التعليم مخاطر أمنية وفوائد في آن واحد. فقد جعل تعرّض الطلاب للإنترنت أكثر عرضة لتهديدات الأمن السيبراني. ولتعزيز الاستخدام طويل الأمد للتكنولوجيا، يجب تثقيف الطلاب حول تهديدات أمن المعلومات وكيفية حماية أنفسهم على الإنترنت. في هذا البحث، نقدّم نتائج دراسة مقطعية حول الوعي بأمن المعلومات بين الطلاب السعوديين. استُخدم استبيان إلكتروني

لجمع البيانات التجريبية، ثم حُلَّت باستخدام نمذجة المعادلات الهيكلية الجزئية للمربعات الصغرى. واستنادًا إلى الأدبيات المتاحة، ركّزنا على أربعة مفاهيم رئيسية: إدارة كلمات المرور، وإدارة البنية التحتية، وإدارة البريد الإلكتروني، والإدراك الأمني. ووفقًا لنتائج هذا الاستطلاع، رأى المشاركون أن إدارة البريد الإلكتروني وإدارة البنية التحتية مهمتان، لكن إدارة كلمات المرور والإدراك الأمني لم يكونا كذلك. كما نُقدّم توصيات لرفع مستوى الوعي بالأمن السيبراني بين الطلاب. ومن المرجح أن تُساعد نتائج هذه الدراسة المؤسسات التعليمية وأولياء الأمور على تثقيف الطلاب حول السلوك الآمن على الإنترنت (Saeed, 2023).

التجارة الإلكترونية عنصر أساسي في رؤية السعودية 2030، التي تتمتع بإمكانات هائلة، لكنها تنطوي أيضًا على خطر الهجمات الإلكترونية. يهدف القطاع المصرفي إلى تعزيز التنمية والابتكار التكنولوجي وزيادة الوصول إلى الخدمات المالية. ويشمل ذلك تعزيز الخدمات المصرفية الرقمية، وزيادة الثقافة المالية، وتوفير التمويل للشركات الصغيرة والمتوسطة. وقد أدى اعتماد القطاع المالي والمصرفي العالمي على التكنولوجيا الجديدة إلى جعله أكثر عرضة للهجمات الإلكترونية. وبالتالي، كان الهدف الرئيسي من هذا البحث هو اكتشاف العناصر التي قد تزيد من الأمن السيبراني بين موظفي البنوك السعودية. وبحث هذه الدراسة في آثار الفائدة المتصورة، والاستعداد التكنولوجي، والتدريب والتطوير، ورضا المستخدم على تبني الأمن السيبراني. كما بحثت في كيفية لعب رضا العملاء دور الوسيط. وقد استخدم نهج بحثي مقطعي في هذه الدراسة. واستُخدمت استبيانات المسح للحصول على بيانات من موظفي البنوك الخاصة السعودية. وبلغ معدل الاستجابة القابل للاستخدام للدراسة 63.14%. وتم تحليل البيانات التي تم جمعها باستخدام Smart PLS 3.3.9. أظهرت النتائج أن الفائدة المُدركة، والتدريب والتطوير، والاستعداد التقني، كانت جميعها مؤشرات قوية على رضا المستخدم. وبالمثل، أثر رضا المستخدم بشكل كبير على نوايا تبني الأمن السيبراني. كما دعمت نتائج الدراسة تأثير نوايا المستخدم الوسيط (Mian, 2023).

المنطلقات النظرية للدراسة:

تعتمد هذه الدراسة على مجموعة من الأسس النظرية والأفكار الإطارية التي تشكل منصة لفهم العلاقة بين الأمن السيبراني واستدامة المبادرات التكنولوجية النامية، مثل:

• أولاً: نظرية الأمن السيبراني

تستند هذه الدراسة إلى العديد من الأسس النظرية التي تُشكل إطاراً فكرياً لتحليل العلاقة بين تبني استراتيجية الأمن السيبراني واستدامة مبادرات التكنولوجيا الناشئة في المملكة العربية السعودية على المدى الطويل. أولى هذه النظريات هي نظرية الأمن السيبراني، التي تُركز على حماية الأنظمة الرقمية والمعلومات الحيوية من التهديدات والهجمات السيبرانية من خلال إدارة المخاطر الرقمية، وتطبيق التدابير الوقائية والاستباقية، والالتزام بالمعايير التنظيمية التي وضعتها الجهات الرسمية، مثل الهيئة الوطنية للأمن السيبراني (Al-Somali, 2024).

• ثانيًا: نظرية استدامة الأعمال

تستند الدراسة أيضًا إلى نظرية استدامة الأعمال، التي تؤكد أن استمرارية المشاريع لا تتحدد فقط بالربحية قصيرة الأجل، بل أيضًا بقدرتها على تحمل العقبات والتكيف مع التغيرات، وخاصةً تلك التي تؤثر على البنية التحتية الرقمية. تُعد الاستدامة التقنية جانبًا مهمًا في ضمان النجاح التشغيلي لتطوير المبادرات التقنية (Sagar, 2023).

• ثالثًا: نظرية ريادة الأعمال التكنولوجية

تستند الدراسة أيضًا إلى نظرية ريادة الأعمال التقنية، التي تصف كيف تُوفر التطورات التكنولوجية الأساس لنجاح ريادة الأعمال. وهذا يعني أن تطبيق تقنيات الحماية والأمن يُعدّ أحد العوامل التي تعزز ثقة السوق، وله تأثير مباشر على نجاح المشروع واستمراره (Maduwanthi, 2022).

• رابعًا: نموذج قبول التكنولوجيا (TAM)

يستخدم البحث أيضًا نموذج قبول التكنولوجيا (TAM)، الذي يصف كيفية قبول الأفراد والمؤسسات لتقنيات التكنولوجيا. ويُفترض أن اعتماد تقنيات الأمن السيبراني يرتبط برؤية مزاياها المتوقعة وسهولة استخدامها، مما يجعلها عنصرًا أساسيًا في قرارات الشركات الناشئة (Schorr, 2023).

• خامسًا: إطار عمل الأمن السيبراني السعودي

يأخذ التقرير في الاعتبار الإطار الوطني السعودي للأمن السيبراني، الذي يغطي السياسات والأنشطة الموضحة في رؤية المملكة 2030. ويُعدّ التحول الرقمي المستدام جانبًا مهمًا من الأجندة الوطنية، ويُعدّ الأمن السيبراني عنصرًا أساسيًا في حماية الاقتصاد الرقمي المزدهر والحفاظ على تنميته واستدامته (Alnasser, 2024).

المنهجية وطرق البحث:

1. تصميم البحث

يعتمد تصميم هذه الدراسة على منهجية وصفية تحليلية، مع دراسة حالة كأساس. وتهدف إلى عرض الوضع الراهن وتقييم أثر تطبيق سياسات الأمن السيبراني على جدوى مبادرات التكنولوجيا الناشئة في المملكة العربية السعودية على المدى الطويل. تتيح هذه البنية فهمًا شاملاً للتفاعلات بين المتغيرات من خلال جمع وتحليل البيانات الواقعية، بهدف التوصل إلى رؤى قابلة للتعميم جزئيًا على مشاريع مماثلة.

2. منهجية دراسة الحالة

يعتمد التقرير على منهجية دراسة الحالة، مع التركيز على عدد محدد من مبادرات التكنولوجيا الناشئة في المملكة العربية السعودية التي طبقت تقنيات الأمن السيبراني. ويسعى هذا الأسلوب إلى تقديم تقييم شامل وكامل لكيفية تأثير هذه

الاستراتيجيات على النجاح التشغيلي والمالي لهذه المشاريع على المدى الطويل، مع التركيز على الجوانب التنظيمية والتقنية والبيئية.

3. تقنيات جمع البيانات

يجمع هذا البحث بيانات كمية من عينة الدراسة، وذلك باستخدام استبيان مغلق ذي مقياس ليكرت خماسي النقاط. صُمم الاستبيان ليشمل مواضيع مثل مستوى تنفيذ خطط الأمن السيبراني، وأشكال التهديدات الرقمية، ومعرفة الإدارة بمخاطر الأمن السيبراني، ومؤشرات الاستدامة التشغيلية والتنظيمية. كما سيتم إجراء مقابلات شبه منظمة مع بعض المسؤولين التنفيذيين في مشاريع التكنولوجيا للحصول على بيانات نوعية تُعزز النتائج الكمية وتُثري الدراسة.

4. استراتيجية أخذ العينات

ستُستخدم عينة غير احتمالية، تُعرف غالبًا بالعينة القصدية. سيتم اختيار عينة من مبادرات التكنولوجيا الناشئة المسجلة لدى الهيئة السعودية للمنشآت الصغيرة والمتوسطة (منشآت) والتي تستخدم البنية التحتية الرقمية لأغراض تشغيلية. تم اختيار العينة بناءً على عوامل مثل توافر أنظمة الأمن السيبراني، وعدد سنوات التشغيل، والاعتماد على الخدمات الرقمية لتوفير أو صيانة منتجاتها.

5. أساليب تحليل البيانات

سيتم تحليل البيانات الكمية المُجمعة من خلال الاستبيان إحصائيًا باستخدام برنامج SPSS، باستخدام الأساليب الإحصائية الوصفية (المتوسطات الحسابية، الانحراف المعياري) والاستدلالية (اختبار t ، تحليل التباين، والانحدار الخطي البسيط والمتعدد) لتحديد العلاقة بين المتغيرات المستقلة (استراتيجيات الأمن السيبراني) والمتغير التابع (استدامة المشروع). سيُستخدم التحليل الموضوعي للكشف عن الأنماط والاختلافات الشائعة في وجهات نظر المشاركين من البيانات النوعية التي جُمعت خلال المقابلات.

6. الصلاحية، والموثوقية، والاعتبارات الأخلاقية

لضمان الصلاحية الداخلية، طُوِّرت أدوات الدراسة باستخدام مراجع أكاديمية مرموقة، وعُرضت على مُحكمين محترفين لتقييم مدى ملاءمتها للأهداف. سيُستخدم معامل ألفا كرونباخ لتقييم الموثوقية وضمان اتساق الاستجابات. وفيما يتعلق بالاعتبارات الأخلاقية، تم اتباع معايير البحث الأخلاقي. وتم إطلاع المشاركين على طبيعة البحث، والحصول على موافقتهم الطوعية. وتم التأكيد على سرية البيانات، والتأكد من أنها لن تستخدم إلا لأغراض البحث العلمي، دون الكشف عن هويات المشاركين أو البيانات المؤسسية.

أدوات الدراسة:

1. دليل المقابلات شبه المنظمة

يُ كان أول هذه الموارد دليلاً للمقابلات شبه المنظمة. أُعدَّ هذا الدليل لتسهيل إجراء مقابلات معمقة مع عدد محدود من مسؤولي الأمن السيبراني والمديرين التنفيذيين العاملين على مبادرات تكنولوجية ناشئة. كان الهدف هو التعرف على تجاربهم ووجهات نظرهم حول واقع تبني استراتيجيات الأمن السيبراني، والتحديات التي يواجهونها، وتأثير هذه الاستراتيجيات على أداء المؤسسة واستدامتها. تُعدّ المقابلات شبه المنظمة مفيدة في استخلاص معلومات نوعية لا تستطيع الأساليب الكمية توفيرها.

2. الاستبيان

يُ أود استخدام استبيان كأداة رئيسية للحصول على بيانات كمية. صُمِّم الاستبيان بمقياس ليكرت خماسي النقاط لتقييم آراء المشاركين حول مدى تبني أساليب الأمن السيبراني وتأثيرها على عوامل الاستدامة الرئيسية. وُزِع الاستبيان على عينة من الموظفين العاملين في مشاريع تكنولوجية ناشئة، وتضمّن بيانات حول مواضيع الدراسة، مثل فعالية التدابير الأمنية، والاستجابة للطوارئ السيبرانية، والأمن التشغيلي، ورضا العملاء، وثقة المستثمرين.

3. قائمة مراجعة الوثائق

بالإضافة إلى ذلك، استُخدمت أداة قائمة تدقيق الوثائق لتقييم جوهر السياسات والخطط والوثائق الداخلية الرسمية في بعض الشركات التقنية. وشملت الوثائق التي تم تحليلها سياسات أمن المعلومات، وسجلات الحوادث الأمنية، وتقارير الأداء،

وخطط الاستدامة. تساعد هذه القائمة على تقييم موثوقية البيانات التي تم الحصول عليها من المشاركين، بالإضافة إلى اكتشاف الممارسات التنظيمية الحقيقية.

4. بروتوكول المراقبة

من أساليب البحث الأخرى تقنية المراقبة، التي طُبقت بشكل روتيني خلال الزيارات الميدانية إلى العديد من الشركات التقنية. راقب هذا البروتوكول سلوك الموظفين أثناء تطبيق اللوائح الأمنية، وتابع إجراءات إدارة البيانات الحساسة، وتتبع الإجراءات المرتبطة بأمن النظام ضد الهجمات الإلكترونية. ووُضعت خطة مراقبة منتظمة لتسجيل هذه النتائج علميًا.

5. برنامج تحليل البيانات

لتحليل البيانات الكمية، استُخدم برنامج SPSS لإجراء تحليلات إحصائية ذات صلة، مثل التكرارات والمتوسط الحسابي والانحراف المعياري، بالإضافة إلى تقييم الارتباطات بين المتغيرات باستخدام تحليل الانحدار. تم تحليل البيانات النوعية من المقابلات والملاحظات موضوعيًا باستخدام أدوات مثل NVivo، مما يسمح للباحث بتحديد الأنماط التفسيرية والمعاني الأساسية وراء إجراءات ومواقف الأمن السيبراني.

حدود الدراسة:

تُعدّ حدود الدراسة سمةً مهمةً يجب تحديدها بوضوح. فهي تُساعد على توضيح نطاق البحث وتحديد الأطر التي أُجريت ضمنها، سواءً من حيث العينة المستهدفة، أو الفترة الزمنية، أو الموقع الجغرافي والمكاني. وفيما يلي القيود المحددة لهذه الدراسة:

• الحدود البشرية

ركّز هذا البحث على الأفراد العاملين في تطوير المبادرات التكنولوجية في المملكة العربية السعودية، بمن فيهم جهات الأمن السيبراني، وكبار المديرين، وموظفو الإدارات التقنية. وقد اختيرت هذه المجموعة لخبرتهم المباشرة في سياسات واستراتيجيات

الأمن السيبراني، مما يجعلهم الأكثر تأهيلاً لتقديم إحصاءات موثوقة حول اعتماد هذه الأساليب وتأثيرها على استدامة المشاريع.

• الحدود الزمنية

أُجريت هذه الدراسة من يناير 2024 إلى يونيو 2025. وشهد هذا العام تقدماً هائلاً في تطبيق السياسات الرقمية والتحول الرقمي كجزء من رؤية المملكة 2030. وقد سمح هذا للباحث بتتبع هذه التغيرات وتأثيرها على المبادرات التكنولوجية بطريقة معاصرة وحديثة.

• الحدود المكانية

أُجريت هذه الدراسة في مدن رئيسية في المملكة العربية السعودية، بما في ذلك الرياض وجدة والدمام، وهي مراكز للتطوير والابتكار التقني. تحتضن هذه المدن غالبية المشاريع التكنولوجية الناشئة، وتوفر بيئة داعمة لريادة الأعمال التقنية، مما يجعلها مناسبة لدراسة تأثير الأمن السيبراني على جدوى هذه المبادرات على المدى الطويل.

المراجع:

- Al-Somali .(2024) .Organizational Cybersecurity Systems and Sustainable Business Performance of Small and Medium Enterprises (SMEs) in Saudi Arabia: The Mediating and Moderating Role of Cybersecurity Resilience and Organizational Culture من الاسترداد من 16(5). <https://www.mdpi.com/2071-1050/16/5/1880>
- Angela Schorr .(2023) .The Technology Acceptance Model (TAM) and its Importance for Digitalization Research: A Review من الاسترداد من 55-65 .
https://www.researchgate.net/publication/372301809_The_Technology_Acceptance_Model_TAM_and_its_Importance_for_Digitalization_Research_A_Review
- Asem Alnasser .(2024) .Navigating Digital Transformation in Alignment with Vision 2030: A Review of Organizational Strategies, Innovations, and Implications in Saudi Arabia . (2)3، 21-29. تم الاسترداد من
https://www.researchgate.net/publication/378544191_Navigating_Digital_Transformation_in_Alignment_with_Vision_2030_A_Review_of_Organizational_Strategies_Innovations_and_Implications_in_Saudi_Arabia
- Ashwag Madkhali .(2023) .Exploring the Role of Information Technology in Supporting Sustainability Efforts in Saudi Arabia من الاسترداد من 15(16) .
<https://www.mdpi.com/2071-1050/15/16/12375>
- Azizah Abdullah Al-Zahrani .(2025) .Success Factors in Achieving Excellence in Cybersecurity (A Case Study of the Kingdom of Saudi Arabia) من الاسترداد من .
<https://www.ijrsp.com/volume/issue-68/3/>
- dga .(2025) . استراتيجيات التحول الرقمي في المملكة العربية السعودية. تم الاسترداد من dga
<https://dga.gov.sa/ar/digital-knowledge/study-of-digital-transformation-strategy>
- dga .(2025) . جاهزية تبني التقنيات الناشئة في الجهات الحكومية لعام 2025م. تم الاسترداد من dga
<https://dga.gov.sa/ar/ET-adoption-readiness-in-government-entities-2025>
- Dinusha Maduwanthi .(2022) .The Emergence of Technopreneurship for Sustainable and Ethical Economic Growth: Theory, Research and Practice من الاسترداد من .
https://www.researchgate.net/publication/361464450_The_Emergence_of_Technopreneurship_for_Sustainable_and_Ethical_Economic_Growth_Theory_Research_and_Practice
- my .(2025) . البيانات التنظيمية التجريبية وأدوات استشراف المستقبل. تم الاسترداد من my
<https://my.gov.sa/ar/content/172>
- my .(2025) . <https://my.gov.sa/ar/content/175>. تم الاسترداد من my

- Nawaf Alhalafi .(2023) .Exploring the Challenges and Issues in Adopting Cybersecurity in Saudi Smart Cities: Conceptualization of the Cybersecurity-Based UTAUT Model . تم الاسترداد من <https://www.mdpi.com/2624-6511/6/3/72> (3)6
- Nisha Rawindaran .(2023) .Enhancing Cyber Security Governance and Policy for SMEs in Industry 5.0: A Comparative Study between Saudi Arabia and the United Kingdom . تم الاسترداد من <https://www.mdpi.com/2673-6470/3/3/14> 231-200
- pwc .(2025) . الاستطلاع الثامن والعشرون لانطباعات الرؤساء التنفيذيين: نتائج المملكة العربية السعودية. تم الاسترداد من <https://www.pwc.com/m1/en/ceo-survey/28th-ceo-survey-middle-east-findings-2025/saudi-arabia-findings-ar.html>
- Sabah Abdullah Al-Somali .(2024) .Organizational Cybersecurity Systems and Sustainable Business Performance of Small and Medium Enterprises (SMEs) in Saudi Arabia: The Mediating and Moderating Role of Cybersecurity Resilience and Organizational Culture تم الاسترداد من <https://www.mdpi.com/2071-1050/16/5/1880> (5)16
- Sahil Sagar .(2023) .Innovation and Sustainability in Business: Navigating the Future Landscape تم الاسترداد من https://www.researchgate.net/publication/377112499_Innovation_and_Sustainability_in_Business_Navigating_the_Future_Landscape
- Saqib Saeed .(2023) .Education, Online Presence and Cybersecurity Implications: A Study of Information Security Practices of Computing Students in Saudi Arabia تم الاسترداد من <https://www.mdpi.com/2071-1050/15/12/9426> (12)15
- Tariq Saeed Mian .(2023) .Exploring Factors to Improve Intentions to Adopt Cybersecurity: A Study of Saudi Banking Sector تم الاسترداد من <https://www.hnjournal.net/en/4-9-8/>
- Wajdi Alhakami .(2024) .Enhancing Cybersecurity Competency in the Kingdom of Saudi Arabia: A Fuzzy Decision-Making Approach تم الاسترداد من https://openurl.ebsco.com/EPDB%3Aagcd%3A9%3A4949817/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Aagcd%3A178454206&crl=c&link_origin=scholar.google.com (2)29
- شيماء إبراهيم. (2024). حصاد 2024.. السعودية تقود مستقبل الشركات الناشئة باستثمارات مليارية. تم الاسترداد من <https://sharikatmubasher.com/media-hub/experts-thoughts/6273>

Mid-Ocean University

College of Management

Department/Major in Entrepreneurship



Research Title

The Impact of Adopting Cybersecurity Strategies on the Sustainability of Tech Startups in the Kingdom of
Saudi Arabia

Student Preparation/ Yasser Hassan Al-Safadi

Student number/ 243000055

Supervision/

Academic Year:

2025