

جامعة ميدأوشن



كلية الإدارة

ماجستير إدارة الأعمال

أثر تطبيق ممارسات الأمن السيبراني على استدامة التحول الرقمي في
المؤسسات السعودية: دراسة ميدانية في ضوء رؤية المملكة 2030

إعداد الطالب/

مشاعل غزاي العتيبي

251002386

إشراف/

أ.د. / الفیصل عبد الحمید

أ.د. / فايز جراد

العام الدراسي:

2025

المقدمة:

تُعد التحولات الرقمية في المؤسسات من أبرز التحولات الاستراتيجية التي تشهدها المنظمات المعاصرة، خاصة في ظل المتغيرات المتسارعة التي يشهدها العالم في مجالات التكنولوجيا الحديثة، وهو ما انعكس بوضوح على بيئة الأعمال في المملكة العربية السعودية. لقد أضحت الرقمنة تمثل ركيزة أساسية في تحقيق التنمية الاقتصادية وتعزيز كفاءة الأداء المؤسسي تماشياً مع رؤية المملكة 2030، حيث تهدف الرؤية إلى تمكين القطاعين العام والخاص من التحول إلى بيئات عمل رقمية تعتمد على التقنيات الحديثة في تقديم الخدمات وتعزيز الإنتاجية. ومع هذا التحول الكبير، باتت قضايا الأمن السيبراني تمثل أولوية قصوى لضمان استدامة الأنظمة الرقمية وفاعلية تطبيق ممارسات التحول الرقمي.

شهدت المؤسسات السعودية توسعاً ملحوظاً في تبني الأنظمة الرقمية، سواء من خلال التوسع في تقديم الخدمات الإلكترونية، أو الاعتماد على التطبيقات الذكية والذكاء الاصطناعي، فضلاً عن استخدام الحوسبة السحابية والتقنيات المالية الرقمية، إلا أن هذا الانفتاح الرقمي صاحبه تصاعد في التهديدات السيبرانية، الأمر الذي دفع المؤسسات إلى إعادة النظر في استراتيجيات حماية البيانات والبنية التحتية الرقمية. ويأتي هذا في وقت تواجه فيه المؤسسات تحديات حقيقية تتعلق بكيفية تحقيق التوازن بين تسريع وتيرة التحول الرقمي من جهة وضمان الحماية الأمنية لأنظمتها من جهة أخرى، بما يحقق الاستدامة الرقمية ويحافظ على كفاءة العمليات المؤسسية (العثامنة والحوري، 2022).

وبالتوازي مع تصاعد وتيرة التحول الرقمي في المملكة العربية السعودية، تبرز تحديات متزايدة تتعلق بمدى نضج واستمرارية هذا التحول داخل المؤسسات، خاصة في ظل التهديدات السيبرانية المتطورة. إذ لم يعد التحول الرقمي مجرد خطوة تقنية لتحسين الخدمات، بل تحول إلى مسار استراتيجي طويل الأمد يتطلب ضمان استمرارية الأداء الرقمي وضمان جاهزية الأنظمة لمواجهة المخاطر السيبرانية. ولهذا، فإن استدامة

التحول الرقمي أصبحت مرهونة بمدى قدرة المؤسسات على ترسيخ ممارسات أمن سيرياني شاملة ومنهجية، تتكامل مع العمليات الرقمية وتدعم الأهداف الاستراتيجية للمؤسسة. من هنا تتبع أهمية هذه الدراسة في تقديم قراءة تحليلية لمدى فاعلية ممارسات الأمن السيرياني في تحقيق الاستدامة الرقمية للمؤسسات السعودية، مع الأخذ بعين الاعتبار الأبعاد الإدارية والتقنية والتنظيمية، بما يعزز من فرص نجاح التحول الرقمي وضمان استمراريته في ظل بيئة عمل رقمية آمنة ومستقرة تتماشى مع التوجهات الوطنية لرؤية المملكة 2030 (عطيه، 2022).

وفي هذا الإطار، برزت أهمية تبني ممارسات فعالة في إدارة الأمن السيرياني، باعتبارها أحد المكونات الأساسية لاستدامة التحول الرقمي في المؤسسات السعودية. إن تطبيق سياسات حماية إلكترونية واضحة، وتطوير برامج توعية أمنية للعاملين، بالإضافة إلى تطوير نظم مراقبة التهديدات والاستجابة السريعة للحوادث السيريانية، تعد من المتطلبات الجوهرية لتحقيق منظومة رقمية مؤمنة وقادرة على التكيف مع التحديات المعاصرة. كما أن التقييم المستمر لمخاطر الأمن السيرياني يمثل أحد الركائز التي تُمكن المؤسسات من التفاعل الفعال مع بيئة العمل الرقمية المتغيرة (دردرة، 2023).

وفي ضوء ما تقدم، تسعى هذه الدراسة إلى تقديم إطار علمي ومنهجي يوضح الدور الجوهري لممارسات الأمن السيرياني في دعم استدامة التحول الرقمي داخل المؤسسات السعودية. وتركز الدراسة على تحليل الأثر الفعلي لهذه الممارسات في تعزيز استقرار الأنظمة الرقمية، وضمان مرونة العمليات التشغيلية، وتقليل مخاطر الانقطاعات السيريانية. كما تهدف إلى اقتراح توصيات تطبيقية تسهم في تطوير سياسات أمن معلومات متكاملة تدعم استمرارية الأعمال وتواكب التوجهات الحديثة التي تتبناها المملكة ضمن رؤية 2030. ومن خلال الدراسة الميدانية، تسعى إلى الوصول إلى نتائج واقعية قابلة للتطبيق تساعد المؤسسات

على تحسين كفاءتها الرقمية، ورفع جاهزيتها السيبرانية بما يضمن تحقيق الأهداف الاستراتيجية بكفاءة واستدامة.

المشكلة البحثية:

تتبع المشكلة البحثية التي تتناولها هذه الدراسة من التحديات المتزايدة التي تواجهها المؤسسات السعودية في ظل التوسع المتسارع في تطبيق التحول الرقمي، حيث أصبحت هذه المؤسسات تعتمد بشكل شبه كلي على البنى التحتية الرقمية لتسيير عملياتها اليومية وتنفيذ مهامها الاستراتيجية. إلا أن هذا التوسع في التحول الرقمي ترافق معه تصاعد ملحوظ في حجم وتعقيد التهديدات السيبرانية التي تستهدف الأنظمة الرقمية، مما يهدد بشكل مباشر استدامة التحول الرقمي ويضع المؤسسات أمام مخاطر حقيقية تتمثل في فقدان البيانات، اضطرابات الأنظمة التشغيلية، وزيادة احتمالات التعرض للهجمات السيبرانية بمختلف أشكالها.

وبالرغم من إدراك المؤسسات السعودية لأهمية التحول الرقمي في تحسين الكفاءة التشغيلية ودعم الاستراتيجيات الوطنية مثل رؤية المملكة 2030، إلا أن الدراسات الميدانية تشير إلى وجود قصور في تطبيق الممارسات الفعالة للأمن السيبراني، سواء من حيث البنية التحتية التكنولوجية أو من حيث تأهيل الكوادر البشرية وتطوير السياسات المؤسسية الخاصة بحوكمة الأمن السيبراني.

كما أن الفجوة البحثية التي تنطلق منها هذه الدراسة تتجسد في قلة الأبحاث التطبيقية التي تربط بشكل مباشر بين ممارسات الأمن السيبراني واستدامة التحول الرقمي في السياق السعودي. فمعظم الأدبيات تركز إما على التحول الرقمي كعملية قائمة بحد ذاتها، أو على الأمن السيبراني كأحد مكونات البنية التحتية التكنولوجية، دون التطرق بشكل متكامل إلى العلاقة التفاعلية بين الأمن السيبراني واستمرارية ونجاح برامج التحول الرقمي على المدى الطويل. كما أن الدراسات القائمة تقتصر إلى التحليل التطبيقي القائم على بيانات

ميدانية من المؤسسات السعودية بمختلف قطاعاتها، الأمر الذي يجعل من الضروري دراسة هذه العلاقة بشكل أعمق وفقاً لطبيعة المؤسسات المحلية وخصائص بيئة الأعمال في المملكة.

لذلك، تهدف هذه الدراسة إلى سد هذه الفجوة من خلال تقديم تحليل ميداني منهجي يستقصي أثر تطبيق ممارسات الأمن السيبراني على تعزيز استدامة التحول الرقمي، مع التركيز على الأبعاد الإدارية والتقنية والتنظيمية التي تسهم في تحقيق استقرار الأنظمة الرقمية وضمان استمرارية الأعمال.

ومن هنا يمكن بلورة مشكلة البحث الحالي في التساؤل الرئيس التالي:

إلى أي مدى تؤثر أبعاد ممارسات الأمن السيبراني (سياسات الحماية الإلكترونية، التدريب والتوعية الأمنية، مراقبة التهديدات والاستجابة للحوادث، التقييم المستمر للمخاطر) في تعزيز استدامة التحول الرقمي داخل المؤسسات السعودية؟

أهمية البحث

أولاً: الأهمية العلمية

• تتبع الأهمية العلمية لهذه الدراسة من تركيزها على قطاع حيوي يتزايد تأثيره في بيئة الأعمال المعاصرة، وهو قطاع التحول الرقمي في المؤسسات السعودية. في ظل التوسع الملحوظ في استخدام التقنيات الحديثة بالمملكة العربية السعودية، لم تتل ممارسات الأمن السيبراني وتأثيرها على استدامة هذا التحول ما تستحقه من الدراسة والبحث العلمي، خاصة في البيئة المحلية. ومن ثم تأتي هذه الدراسة لسد هذه الفجوة المعرفية من خلال ربط الأبعاد السيبرانية بجهود التحول الرقمي.

- تقدم الدراسة إضافة علمية بارزة من خلال استكشاف العلاقة بين تطبيق ممارسات الأمن السيبراني واستدامة التحول الرقمي، عبر دمج مفاهيم التحول المؤسسي الرقمي مع الأطر التنظيمية والتكنولوجية للأمن السيبراني، لتكوين رؤية متكاملة حول حماية الأنظمة الرقمية وضمان استمراريته بكفاءة.
- تساهم الدراسة في معالجة قصور معرفي قائم في الدراسات الأكاديمية السعودية، حيث نفتقر غالبية الأدبيات المحلية إلى تحليلات تطبيقية تقيس الأثر الفعلي لممارسات الحماية الإلكترونية على نجاح استراتيجيات التحول الرقمي في بيئات الأعمال السعودية.
- تبرز الأهمية العلمية للدراسة في تبنيها منهجاً ميدانياً يعتمد على بيانات واقعية من بيئات مؤسسية سعودية، ما يضيف على نتائجها مصداقية عالية يمكن أن تستند إليها دراسات لاحقة في مجالات التحول الرقمي، أمن المعلومات، وتحقيق استدامة الأداء المؤسسي في القطاعين العام والخاص.
- تساهم الدراسة في تطوير معرفة علمية تطبيقية تساهم في بناء نماذج قياس فعالة يمكن الاستفادة منها في تقييم كفاءة التحول الرقمي، من خلال الربط بين الاستدامة المؤسسية ومستوى تبني ممارسات الأمن السيبراني داخل المؤسسات الوطنية.

ثانيًا: الأهمية العملية

- تكتسب الدراسة أهمية عملية واضحة كونها تتعامل مع تحدٍ حقيقي تواجهه المؤسسات السعودية، يتمثل في تزايد المخاطر السيبرانية بالتوازي مع جهود التحول الرقمي، ما يعرض الاستدامة المؤسسية للخطر في حال غياب استراتيجيات أمنية متكاملة.
- تقدم الدراسة أدوات عملية للمديرين التنفيذيين وقادة التحول الرقمي في المؤسسات السعودية من خلال اقتراح سياسات وقائية قائمة على أفضل الممارسات العالمية، مع تكييفها لخصوصية البيئة السعودية، بما يضمن تحقيق تحول رقمي آمن ومستدام.

• تساعد نتائج الدراسة صنّاع القرار في المؤسسات السعودية على تصميم أطر تنظيمية وتشغيلية متكاملة تجمع بين الحماية السيبرانية واستمرارية العمل، بما يعزز الأداء المؤسسي ويحسن الثقة الرقمية لدى المستفيدين والعملاء.

• تساهم الدراسة في خفض المخاطر التقنية والتشغيلية التي تواجه المؤسسات أثناء التحول الرقمي، عبر توجيهها نحو ممارسات أمنية فعالة تساعد على تقليل فرص التوقف المفاجئ، وحماية البيانات، وضمان كفاءة التشغيل الإلكتروني.

• تدعم الدراسة القطاع الخاص في المملكة العربية السعودية بمرجع علمي تطبيقي يساعده في تعزيز تنافسيته، من خلال دمج البعد السيبراني ضمن خطط التحول الرقمي، بما ينعكس إيجاباً على مرونة الأعمال واستدامة تقديم الخدمات.

• تتسجم الدراسة مع مستهدفات رؤية المملكة 2030، خاصة في جوانب تطوير الاقتصاد الرقمي وتحقيق مجتمع معلوماتي آمن، حيث تساهم في تعزيز استدامة المشاريع الرقمية ورفع جاهزية المؤسسات السعودية للتعامل مع التهديدات السيبرانية المستجدة.

أهداف البحث:

الهدف الرئيسي:

يسعى هذا البحث إلى تحليل أثر أبعاد ممارسات الأمن السيبراني على استدامة التحول الرقمي داخل المؤسسات السعودية في ضوء رؤية المملكة 2030.

1) الأهداف الفرعية:

(2) التعرف على أثر سياسات وإجراءات الحماية الإلكترونية في دعم استمرارية العمليات الرقمية داخل المؤسسات.

(3) قياس أثر التدريب والتوعية الأمنية على تحسين جاهزية الموارد البشرية لمواجهة التهديدات السيبرانية أثناء التحول الرقمي.

(4) دراسة تأثير نظم مراقبة التهديدات والاستجابة للحوادث في الحد من الأعطال الرقمية ودعم استدامة الأنظمة الإلكترونية.

(5) توضيح أثر التقييم المستمر لمخاطر الأمن السيبراني على تعزيز مرونة الأنظمة الرقمية وتحقيق استدامة التحول الرقمي.

تساؤلات البحث:

السؤال الرئيسي:

إلى أي مدى تؤثر أبعاد ممارسات الأمن السيبراني (سياسات الحماية الإلكترونية، التدريب والتوعية الأمنية، مراقبة التهديدات والاستجابة للحوادث، التقييم المستمر للمخاطر) في تعزيز استدامة التحول الرقمي داخل المؤسسات السعودية؟

الأسئلة الفرعية:

- (1) ما دور سياسات وإجراءات الحماية الإلكترونية في ضمان استقرار واستدامة الأنظمة الرقمية؟
- (2) كيف يساهم التدريب والتوعية الأمنية في رفع كفاءة الكوادر المؤسسية لمواكبة التحول الرقمي بأمان؟

3) إلى أي حد تسهم نظم مراقبة التهديدات والاستجابة للحوادث في تقليل الانقطاعات التشغيلية

الرقمية؟

4) ما أثر التقييم المستمر لمخاطر الأمن السيبراني في تحقيق مرونة واستدامة الأداء المؤسسي

الرقمي؟

فرضيات البحث:

الفرضية الرئيسية:

لا توجد علاقة ذات دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين أبعاد ممارسات الأمن السيبراني (سياسات الحماية، التدريب والتوعية، مراقبة التهديدات، تقييم المخاطر) واستدامة التحول الرقمي في المؤسسات السعودية.

الفرضيات الفرعية:

1) لا توجد علاقة ذات دلالة إحصائية بين سياسات الحماية الإلكترونية وتحقيق استدامة التحول الرقمي.

2) لا توجد علاقة ذات دلالة إحصائية بين التدريب والتوعية الأمنية ودعم الاستدامة الرقمية المؤسسية.

3) لا توجد علاقة ذات دلالة إحصائية بين نظم مراقبة التهديدات والاستجابة للحوادث وتحقيق استمرارية الأنظمة الرقمية.

4) لا توجد علاقة ذات دلالة إحصائية بين تقييم المخاطر السيبرانية المستمر وضمان استدامة التحول الرقمي داخل المؤسسات السعودية.

الدراسات السابقة:

أولاً: الدراسات العربية

دراسة العثامنة والحوري (2022):

هدفت الدراسة إلى التعرف على أثر التحول الرقمي على الاستدامة في المنظمات الصناعية المدرجة في بورصة عمان. استخدمت الدراسة المنهج الوصفي التحليلي من خلال توزيع استبانة على عينة من المديرين والعاملين في الإدارات العليا والوسطى في المنظمات الصناعية. تناولت الدراسة أبعاد التحول الرقمي مثل الأتمتة، البنية التحتية التكنولوجية، والقدرات الرقمية وتأثيرها على تحقيق الاستدامة بأبعادها الاقتصادية والاجتماعية والبيئية. توصلت النتائج إلى وجود علاقة إيجابية ذات دلالة إحصائية بين التحول الرقمي وتحقيق الاستدامة، وأكدت على أهمية توظيف التقنيات الرقمية في تطوير العمليات الصناعية وتحقيق الكفاءة وتقليل الهدر في الموارد. وأوصت الدراسة بضرورة تعزيز الاستثمارات في البنية التحتية الرقمية وتطوير الكفاءات الرقمية لدى العاملين لتعزيز استدامة المنظمات الصناعية في بيئة تنافسية متغيرة.

دراسة عطية (2022):

سعت الدراسة إلى فحص أثر تطبيق التحول الرقمي على تحسين الأداء الاستراتيجي للشركات الصناعية المقيدة بالبورصة المصرية. اعتمدت الدراسة على المنهج الكمي التحليلي باستخدام استبانة لجمع البيانات من مسؤولي الإدارات العليا بالشركات الصناعية. ركزت الدراسة على ثلاثة أبعاد رئيسية للتحول الرقمي وهي استخدام الأنظمة الذكية، تطوير المنصات الرقمية، وتطبيقات التحليلات التنبؤية، وقياس تأثيرها على محاور الأداء الاستراتيجي كتحقيق النمو، تعزيز القدرة التنافسية، وتحقيق الاستدامة المالية. بينت النتائج وجود تأثير إيجابي واضح للتحول الرقمي على تحسين الأداء الاستراتيجي، لا سيما في مجال مرونة

القرارات وتحقيق الكفاءة التشغيلية. وأوصت الدراسة بضرورة وضع خطط تحول رقمي متكاملة وربطها بخطط الأداء الاستراتيجي لتحقيق أفضل النتائج في بيئة الأعمال الصناعية.

دراسة جربوعة وبوطمين (2023):

تناولت الدراسة موضوع الفضاء الرقمي وتأثيراته على قضايا الأمن السيبراني، حيث ركزت على تحليل التحديات التي تواجه المؤسسات في البيئة الرقمية الحديثة. تم الاعتماد على المنهج الوصفي التحليلي من خلال تحليل الأدبيات الحديثة المتعلقة بالهجمات السيبرانية وتطور تقنيات الحماية. أوضحت الدراسة أن التوسع في استخدام الفضاء الرقمي يقترن بزيادة المخاطر المتعلقة بالاختراقات والجرائم الإلكترونية، مما يستدعي تطوير أنظمة حماية متقدمة. خلصت النتائج إلى أن الأمن السيبراني أصبح أحد الركائز الأساسية لاستمرارية الأعمال في العصر الرقمي، وأوصت الدراسة بضرورة تطوير السياسات الوطنية للأمن السيبراني وتدريب الكوادر البشرية على تقنيات الحماية الرقمية الحديثة لضمان أمن المعلومات وتقليل مخاطر الفضاء الإلكتروني على المؤسسات.

الدراسات الأجنبية:

دراسة Al-Somali et al (2024):

تناولت هذه الدراسة العلاقة بين أنظمة الأمن السيبراني المؤسسية والأداء المستدام للمؤسسات الصغيرة والمتوسطة في المملكة العربية السعودية، مع التركيز على الأدوار الوسيطة والتعديلية لكل من مرونة الأمن السيبراني والثقافة التنظيمية. استخدمت الدراسة المنهج الكمي من خلال استبيانات شملت عينات من إدارات تقنية المعلومات وإدارات الجودة في المؤسسات الصغيرة والمتوسطة. أظهرت النتائج وجود علاقة إيجابية قوية بين فعالية أنظمة الأمن السيبراني والتحسين في الأداء المستدام، مع إبراز أهمية مرونة المؤسسة في

مواجهة الهجمات السيبرانية وأثر الثقافة التنظيمية في تعزيز هذا التأثير. توصي الدراسة بضرورة تبني استراتيجيات لتعزيز مرونة نظم الحماية السيبرانية وتطوير ثقافة مؤسسية داعمة للأمن السيبراني لتحقيق استدامة الأعمال في بيئات الأعمال الرقمية.

دراسة Alnasser et al (2024):

هدفت الدراسة إلى استعراض استراتيجيات التحول الرقمي في المملكة العربية السعودية ودورها في تحقيق مستهدفات رؤية 2030، مع تقييم الابتكارات التنظيمية وانعكاساتها على بيئة الأعمال. اعتمدت الدراسة على تحليل مراجعات الأدبيات الحديثة والدراسات الاستقصائية لمؤسسات سعودية في مختلف القطاعات. أظهرت النتائج أن التحول الرقمي بات جزءاً رئيسياً من التوجهات الاستراتيجية للمؤسسات السعودية، وساهم في تعزيز كفاءة الأعمال وزيادة المرونة التنافسية. أكدت الدراسة على أهمية تكامل استراتيجيات التحول الرقمي مع خطط التطوير المؤسسي والابتكار، مع وجود بعض التحديات المتعلقة بالبنية التحتية الرقمية. وأوصت بزيادة الاستثمارات في التحول الرقمي وتطوير المهارات الرقمية للكوادر العاملة.

دراسة Saeed et al (2023):

ناقشت الدراسة التحديات المتعلقة بالتحول الرقمي وتأثير مشكلات الأمن السيبراني على مرونة الأعمال، من خلال استعراض قضايا معاصرة وتقديم توصيات عملية. استخدمت الدراسة أسلوب تحليل الأدبيات الحديثة مع التركيز على الشركات العاملة في الأسواق الخليجية. كشفت النتائج عن تزايد التهديدات الإلكترونية مع توسع التحول الرقمي، وتأثيرها السلبي على استمرارية الأعمال في حال غياب استراتيجيات حماية فعالة. أشارت الدراسة إلى أن معالجة قضايا الأمن السيبراني تعد أمراً حاسماً لضمان نجاح التحول

الرقمي. وأوصت بوضع أطر تنظيمية صارمة، وتطوير بنى تحتية رقمية مرنة، وتعزيز وعي العاملين بقضايا الأمن الرقمي.

دراسة Alhejaili (2024):

استعرضت الدراسة الأطر القانونية المنظمة للأمن السيبراني في قطاع التجارة الإلكترونية بالمملكة العربية السعودية، مع تقييم مدى فاعلية هذه الأطر في تحقيق الحماية للمستهلكين والشركات. استخدمت الدراسة المنهج التحليلي القانوني، مع دراسة مقارنة بين التشريعات السعودية والدولية. أظهرت النتائج أن المملكة حققت تقدماً ملموساً في تطوير التشريعات السيبرانية، إلا أن هناك حاجة لمزيد من التعديلات لتعزيز مرونة النظام القانوني مع متغيرات الفضاء الرقمي. أكدت الدراسة على أهمية التحديث المستمر للقوانين، وزيادة التنسيق بين الجهات الرقابية، وتكثيف برامج التوعية لضمان بيئة إلكترونية آمنة ومستدامة في التجارة الإلكترونية.

دراسة Shehadeh (2024):

ركزت هذه الدراسة على الدور المحوري الذي تلعبه التحولات الرقمية في تعزيز ممارسات الأعمال المستدامة، حيث تناولت كيف يمكن للتحول الرقمي أن يساهم في تحسين الكفاءة البيئية والاقتصادية للشركات. اعتمدت الدراسة على منهج تحليلي لمجموعة من التجارب العالمية في قطاعات مختلفة، واستعرضت التأثيرات الإيجابية للتحول الرقمي على تحسين استهلاك الموارد وتقليل الانبعاثات الكربونية وتعزيز الشفافية التشغيلية. أوضحت النتائج أن التحول الرقمي لا يقتصر فقط على تحديث التكنولوجيا، بل يشكل إطاراً متكاملاً لتحقيق التنمية المستدامة على مستوى المؤسسات. وأوصت بضرورة تبني استراتيجيات رقمية مستدامة تدمج الابتكار التكنولوجي مع الأهداف البيئية والاجتماعية لضمان استمرارية الأعمال.

دراسة Kosnikov et al (2024):

ناقشت الدراسة العلاقة بين الأمن السيبراني والتنمية المستدامة للاقتصاد الرقمي، موضحة كيف يسهم الأمن المعلوماتي في استقرار البيئة الرقمية ويدعم استدامة الأنشطة الاقتصادية. اعتمدت الدراسة على تحليل بيانات من قطاعات مختلفة في الاقتصاد الرقمي، وأشارت إلى أن التهديدات السيبرانية تمثل أحد أكبر المخاطر أمام تحقيق تنمية اقتصادية رقمية مستدامة. بيّنت النتائج أن وجود بنية تحتية قوية للأمن السيبراني يؤدي إلى تحسين بيئة الأعمال الرقمية، وزيادة ثقة المستثمرين والمستهلكين، مما ينعكس إيجاباً على الاستدامة الاقتصادية. وأوصت الدراسة بضرورة توسيع الاستثمارات في مجال الأمن السيبراني كأحد الركائز الاستراتيجية لضمان تطور رقمي مستدام.

دراسة Sachdeva and Sharma (2024):

استهدفت الدراسة تحليل دور التحول الرقمي المسؤول في بناء مجتمع مستدام، من خلال استعراض مبادرات رقمية تساهم في دعم الأهداف التنموية. ركزت الدراسة على النماذج التطبيقية للتحول الرقمي في مجالات الصحة والتعليم والخدمات المجتمعية، وأظهرت النتائج أن الاستخدام الواعي والمسؤول للتكنولوجيا الرقمية يساهم في تحسين الوصول إلى الخدمات، وتحقيق العدالة الاجتماعية، وتقليل الفجوة الرقمية. أشارت النتائج إلى ضرورة تطوير سياسات تدعم التحول الرقمي المتوازن، الذي يراعي الأبعاد الاجتماعية والبيئية إلى جانب الأبعاد الاقتصادية. خلصت الدراسة إلى أهمية التكامل بين التقنيات الحديثة ومبادئ المسؤولية الاجتماعية لتحقيق تنمية مجتمعية شاملة ومستدامة.

أوجه التشابه والاختلاف بين الدراسات السابقة والدراسة الحالية:

أوجه التشابه:

- تركّز كل من الدراسات السابقة والدراسة الحالية على العلاقة التكاملية بين التحول الرقمي والأمن السيبراني، حيث تتفق الدراسات في إبراز أهمية تبني ممارسات أمن المعلومات كعامل جوهري لاستدامة الأنشطة الرقمية ونجاح مبادرات التحول الرقمي.
- تشترك الدراسات في التركيز على الأبعاد الاستراتيجية للأمن السيبراني، حيث لا تقتصر على الجوانب التقنية فقط، بل تدمج عناصر مثل الثقافة المؤسسية والسياسات الحكومية وأثرها على استدامة الأداء المؤسسي في البيئة الرقمية.
- تتقاطع جميع الدراسات مع الدراسة الحالية في أهمية مواكبة التغيرات السريعة في البيئة التكنولوجية، حيث تؤكد على ضرورة مواءمة خطط الأمن السيبراني مع الابتكارات الرقمية، لضمان حماية الأنظمة وتحقيق تنمية مستدامة.

أوجه الاختلاف:

- تركّز الدراسات السابقة غالباً على بيانات متنوعة تشمل الاقتصاد الرقمي العالمي، المؤسسات المالية، أو القطاعات الصناعية، بينما تنفرد الدراسة الحالية بالتركيز على المؤسسات السعودية في سياق رؤية المملكة 2030، مما يمنحها بعداً محلياً أكثر وضوحاً.
- تعتمد بعض الدراسات السابقة على تحليلات نظرية أو مراجعات أدبية دون دراسة ميدانية معمقة، في حين تتميز الدراسة الحالية بمنهج ميداني تطبيقي باستخدام أدوات جمع بيانات مباشرة، ما يعزز مصداقية النتائج المرتبطة بالسياق السعودي.

- تتناول الدراسة الحالية العلاقة بين ممارسات الأمن السيبراني واستدامة التحول الرقمي بشكل مباشر وتطبيقي، بينما تكتفي الدراسات السابقة غالباً بمناقشة كل منهما على حدة أو من خلال نظرة نظرية، دون اختبار الأثر المباشر بين المتغيرين في بيئة مؤسسية محددة.

المنطلقات النظرية للبحث:

1- الأمن السيبراني:

يُعرف الأمن السيبراني بأنه مجموعة من الأنشطة والإجراءات التي تهدف إلى حماية الأنظمة الإلكترونية، والشبكات، والبيانات الرقمية من الهجمات السيبرانية والمخاطر الإلكترونية المحتملة، بما يضمن سلامة المعلومات وحماية البنية التحتية الرقمية للمؤسسة. يتضمن الأمن السيبراني الأطر التنظيمية والتقنية والبشرية التي تعمل على تعزيز الحماية وتقليل نقاط الضعف الإلكترونية (العثامنة والحوري، 2022).

أبعاد الأمن السيبراني:

- الالتزام بسياسات الأمن المعلوماتي.
- حماية الأنظمة التقنية من الاختراقات والهجمات الخبيثة.
- تعزيز ثقافة الوعي الأمني بين الأفراد.
- تطوير خطط الاستجابة للطوارئ والهجمات السيبرانية.

2- التحول الرقمي:

يقصد بالتحول الرقمي عملية دمج التقنيات الرقمية الحديثة ضمن البنية المؤسسية بهدف تحسين الأداء التشغيلي، وتطوير الخدمات، وتعزيز القدرة التنافسية. يُعد التحول الرقمي منهجاً استراتيجياً يركز على إعادة

تصميم العمليات المؤسسية من خلال استغلال التقنيات الرقمية بما يتماشى مع متطلبات العصر الرقمي (عطيه، 2022).

أبعاد التحول الرقمي:

- تبني التقنيات الرقمية في العمليات التشغيلية.
- تنمية المهارات والقدرات الرقمية للموظفين.
- تطوير بيئة العمل من خلال أتمتة العمليات.
- تحديث الخدمات المقدمة للعملاء عبر القنوات الرقمية.

3- استدامة التحول الرقمي:

تُشير استدامة التحول الرقمي إلى قدرة المؤسسات على الاستمرار في تبني وتطوير تقنيات التحول الرقمي بطريقة منهجية تحقق الفاعلية على المدى البعيد، مع مراعاة الحفاظ على الموارد المالية والتشغيلية وتخفيف المخاطر المحتملة. تهدف الاستدامة الرقمية إلى تحقيق توازن بين التقدم التكنولوجي والاستمرارية المؤسسية (دريرة، 2023).

أبعاد استدامة التحول الرقمي:

- الحفاظ على كفاءة واستمرارية الأنظمة الرقمية.
- التأقلم المستمر مع التطورات التكنولوجية.
- تحسين كفاءة الإنفاق على مشروعات التحول الرقمي.
- خفض معدلات الفشل في المبادرات الرقمية وتعزيز النتائج المستدامة.

منهج البحث:

تعتمد هذه الدراسة على المنهج الوصفي التحليلي بهدف دراسة وتحليل أثر تطبيق ممارسات الأمن السيبراني بأبعاده المختلفة على استدامة التحول الرقمي في المؤسسات السعودية، وذلك في ضوء مستهدفات رؤية المملكة 2030. يستند هذا المنهج إلى تقديم وصف دقيق لطبيعة الممارسات الأمنية المعتمدة داخل المؤسسات السعودية، وتحليل علاقاتها بمؤشرات الاستدامة الرقمية، مع التركيز على ضمان استمرارية الخدمات الرقمية وتقليل المخاطر المرتبطة بالهجمات السيبرانية. يسهم المنهج الوصفي التحليلي في تحقيق فهم شامل للعلاقة التفاعلية بين الأمن السيبراني والتحول الرقمي، واستخلاص استنتاجات علمية يمكن البناء عليها في تطوير السياسات المؤسسية.

تعتمد الدراسة على جمع البيانات الميدانية باستخدام استبانة علمية تم تصميمها لتناسب طبيعة عمل الكوادر التقنية والإدارية بالمؤسسات السعودية التي تعتمد بشكل كبير على النظم الرقمية. تستهدف الاستبانة قياس مستوى تطبيق ممارسات الأمن السيبراني من خلال أربعة أبعاد رئيسية، وهي: إدارة المخاطر السيبرانية، جاهزية البنية التحتية الأمنية، برامج التوعية والتدريب الأمني، ووجود سياسات ولوائح تنظيمية واضحة. كما تقيس الاستبانة تأثير هذه الأبعاد على استدامة التحول الرقمي، من خلال مؤشرات تشمل استمرارية العمليات الرقمية، تقليل التعرض للمخاطر الإلكترونية، وضمان الجاهزية التشغيلية للأنظمة الرقمية.

تم توزيع الاستبانة على عينة قصدية من العاملين في إدارات تقنية المعلومات، الأمن السيبراني، والتحول الرقمي داخل مجموعة من المؤسسات الحكومية والخاصة، لضمان جمع بيانات متنوعة تمثل طبيعة المؤسسات السعودية. كما تم اعتماد مقياس ليكرت الخماسي لقياس درجة موافقة المبحوثين على فقرات الاستبانة، بما يتيح تقييم الأثر بطريقة كمية قابلة للتحليل الإحصائي.

وبجانب ذلك، تم دعم الجانب الكمي بإجراء مقابلات شبه منظمة مع مختصين في الأمن السيبراني ومديري التحول الرقمي داخل المؤسسات السعودية، بهدف استكشاف التحديات التي تواجه تطبيق الممارسات الأمنية ودورها في تعزيز استدامة التحول الرقمي من واقع بيئة العمل المحلية.

مصادر البيانات في الدراسة:

■ المصادر الثانوية: تشمل الأبحاث العلمية والدراسات الأكاديمية المرتبطة بالأمن السيبراني، التحول الرقمي، تقارير الجهات الحكومية السعودية المعنية، وأدلة تنظيمية صادرة عن الهيئات الرقابية.

■ المصادر الأولية: تتمثل في البيانات الميدانية التي يتم جمعها مباشرة من العاملين في المؤسسات السعودية عبر الاستبانات والمقابلات.

أدوات الدراسة والأساليب الإحصائية:

■ الإحصاء الوصفي:

- حساب التكرارات والنسب المئوية لتحليل خصائص المشاركين واتجاهاتهم تجاه ممارسات الأمن السيبراني.
- حساب المتوسطات والانحرافات المعيارية لقياس مدى انتشار ممارسات الأمن السيبراني وتأثيرها على استدامة التحول الرقمي.

■ الإحصاء التحليلي:

- تحليل الانحدار الخطي البسيط لدراسة أثر كل بعد من أبعاد الأمن السيبراني على استدامة التحول الرقمي بشكل منفرد.

- تحليل الانحدار المتعدد لقياس التأثير المجمع لجميع الأبعاد على استدامة التحول الرقمي.

- اختبارات التوزيع الطبيعي للتأكد من صلاحية البيانات لاستخدام الأساليب الإحصائية الاستدلالية.

نموذج الدراسة:

يعتمد نموذج الدراسة على تحديد العلاقة بين متغيرين رئيسيين:

■ المتغير المستقل: ممارسات الأمن السيبراني ويتضمن أربعة أبعاد:

- إدارة المخاطر السيبرانية.
- جاهزية البنية التحتية الرقمية.
- برامج التوعية والتدريب الأمني.
- السياسات واللوائح التنظيمية.

■ المتغير التابع: استدامة التحول الرقمي، ويتم قياسها من خلال:

- استمرارية الأنظمة والخدمات الرقمية.
- تقليل احتمالات التعرض للتهديدات السيبرانية.
- تعزيز مرونة الأعمال الرقمية.
- ضمان التوسع الرقمي الآمن وفق خطط التحول المؤسسي.

حدود الدراسة:

■ الحدود الزمانية: تنحصر الدراسة في عام 2025 لمواكبة أحدث التطورات في استراتيجيات التحول

الرقمي والسياسات الوطنية السعودية للأمن السيبراني.

■ الحدود المكانية: تركز على المؤسسات السعودية بمختلف أنواعها، الحكومية والخاصة، التي تتبنى برامج

تحول رقمي نشطة في مدن رئيسية مثل الرياض وجدة والخبر.

■ الحدود الموضوعية: تقتصر على دراسة أثر ممارسات الأمن السيبراني على استدامة التحول الرقمي فقط، دون تناول جوانب أخرى مثل العائد الاستثماري أو رضا المستخدمين عن الخدمات الرقمية.

قائمة المراجع:

- العثامنة، فرح فيصل محمد بهاء، و الحوري، سليمان إبراهيم شلاش. (2022). أثر التحول الرقمي على الاستدامة في المنظمات الصناعية المدرجة في بورصة عمان (رسالة ماجستير غير منشورة). جامعة آل البيت، المفرق. مسترجع من

<http://search.mandumah.com/Record/1306029>

- عطيه، نورهان صبحي محمد. (2022). أثر تطبيق التحول الرقمي على تحسين الأداء الاستراتيجي للشركات الصناعية المقيدة بالبورصة المصرية. المجلة العلمية للدراسات والبحوث المالية والإدارية، مج13، ع2 ، 500 - 524. مسترجع من

<http://search.mandumah.com/Record/1290938>

- جربوعة، عادل، و بوطمين، عبدالجبار. (2023). الفضاء الرقمي والأمن السيبراني. مجلة العلوم الإنسانية، مج34، ع3 ، 453 - 464. مسترجع من

<http://search.mandumah.com/Record/1418616>

- دردة، السعيد عبدالصالحين محمد. (2023). الذات السيبرانية: تصور عاملي للمفهوم في مستقبل التحول الرقمي. علم النفس، س36، ع139 ، 81 - 99. مسترجع من

<http://search.mandumah.com/Record/1470585>

- Al-Somali, S. A., Saqr, R. R., Asiri, A. M., & Al-Somali, N. A. (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. Sustainability, 16(5), 1880.

<https://doi.org/10.3390/su16051880>

- Alnasser, A., Al Ghofaili, O. R., Ali, M., & AlZaidan, I. Z. (2024). Navigating Digital Transformation in Alignment with Vision 2030: A Review of Organizational Strategies, Innovations, and Implications in Saudi Arabia. *Journal of Knowledge Learning and Science Technology*, 3(2), 21–29. <https://doi.org/10.60087/jklst.vol3.n2.p29>
- Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. 23. <https://doi.org/10.3390/s23156666>
- Alhejaili, M. O. M. (2024). Securing the Kingdom's e-commerce frontier: Evaluation of Saudi Arabia's cybersecurity legal frameworks. *Journal of Governance and Regulation*, 13(2, special issue), 275–286. <https://doi.org/10.22495/jgrv13i2siart4>
- Shehadeh, M. (2024). Digital Transformation: A Catalyst for Sustainable Business Practices (pp. 29–45). Emerald (MCB UP). <https://doi.org/10.1108/978-1-83753-106-620241003>
- Kosnikov, S. N., Zolkin, A. L., Artemyev, N. V., & Lepshokova, A. N. (2024). Cybersecurity as a factor of sustainable development of the digital

economy. *Èkonomika i Upravlenie: Problemy, Rešeniâ*, 12/15(153), 221–229. <https://doi.org/10.36871/ek.up.p.r.2024.12.15.026>

- Sachdeva, T., & Sharma, R. (2024). Responsible Digital Transformation For A Sustainable Society. *Proceeding of International Conference on Science, Health, and Technology*, 83–89. <https://doi.org/10.47701/icohetech.v5i1.4132>

MidOcean University

College of Management

Master of Business Administration



**"The Impact of Implementing Cybersecurity Practices on the
Sustainability of Digital Transformation in Saudi Institutions: A Field
Study in Light of Saudi Vision 2030"**

Preparation:

Mashael Ghazay Alotaibi

251002386

Supervision:

Dr. Al faisal Abdelhameed Mohamed

Dr. Fayez Ali Jrad

1447 – 2025