

أثر الأمن السيبراني على نجاح و كفاءة إدارة المشاريع الرقمية : دراسة تطبيقية

وفاء ماجد حسين البرقوني

مشروع تخرج- ١
كلية الإدارة- جامعة ميدأوشن

إشراف

د. عبد الرحيم نادر
عضو هيئة التدريس- كلية الإدارة- جامعة ميدأوشن

٢٠٢٦م

جدول المحتويات

٣	١. الفصل الأول: الإطار العام للدراسة
٤	١,١. المقدمة:
٥	١,٢. مشكلة الدراسة
٥	١,٢,١. فجوات على المستوى النظري
٥	١,٢,٢. فجوات على المستوى التطبيقي
٦	١,٣. أهمية الدراسة
٦	١,٣,١. على المستوى النظري:
٦	١,٣,٢. على المستوى التطبيقي:
٦	١,٤. أسئلة الدراسة
٧	١,٥. أهداف الدراسة
٧	١,٦. فرضيات الدراسة
٨	١,٧. نموذج الدراسة
٩	١,٨. منهجية الدراسة
١١	١,٩. الدراسة الميدانية
١٤	١,١٠. مخطط المشروع المقترح
١٦	٢. الفصل الثاني: الدراسات السابقة
١٧	٢,١. المقدمة:
١٧	٢,٢. المتغير المستقل
١٧	٢,٣. المتغير التابع
١٨	٢,٤. العلاقة بين المتغير المستقل والمتغير التابع
١٨	٢,٥. الخاتمة
١٩	قائمة المراجع

١. الفصل الأول: الإطار العام للدراسة

١,١. المقدمة:

في ظل التطور الرقمي المتسارع الذي يشهده العالم، أصبحت إدارة المشاريع من الركائز الأساسية التي تعتمد عليها المؤسسات لتحقيق أهدافها بكفاءة وفعالية، خاصة في ظل التنافس المتزايد والتغيرات المستمرة في بيئة الأعمال. وقد ساهم التقدم التكنولوجي في تحويل العديد من المشاريع إلى بيئات رقمية تعتمد بشكل كبير على الأنظمة الإلكترونية والتطبيقات الحديثة.

ومع هذا التحول الرقمي، ظهرت تحديات جديدة تواجه إدارة المشاريع، من أبرزها المخاطر المرتبطة بالأمن السيبراني، والتي تشمل الهجمات الإلكترونية واختراق الأنظمة وتسريب البيانات. إذ يمكن أن تؤدي هذه التهديدات إلى تعطيل سير العمل، وزيادة التكاليف، والتأثير سلبيًا على جودة مخرجات المشروع، مما ينعكس بشكل مباشر على نجاحه.

ويكتسب موضوع الأمن السيبراني أهمية متزايدة في ظل الاعتماد الكبير على التكنولوجيا، حيث أصبح عنصرًا أساسيًا في حماية معلومات المشاريع وضمان استمراريتها. كما أن دمج ممارسات الأمن السيبراني ضمن عمليات إدارة المشاريع يساهم في تقليل المخاطر وتعزيز كفاءة الأداء وتحقيق الأهداف المرجوة.

ومن هذا المنطلق، تهدف هذه الدراسة إلى التعرف على أثر الأمن السيبراني على نجاح وكفاءة إدارة المشاريع الرقمية، من خلال تحليل دوره في تقليل المخاطر وتحسين جودة الأداء، بما يساهم في دعم استمرارية المشاريع وتحقيق نتائج أكثر فاعلية.

١,٢. مشكلة الدراسة

في ظل التوسع الكبير في استخدام الأنظمة الرقمية في إدارة المشاريع، أصبحت المؤسسات تعتمد بشكل متزايد على التكنولوجيا في تخطيط وتنفيذ ومتابعة أعمالها. وعلى الرغم من هذا التطور، إلا أن العديد من المشاريع لا تزال تواجه تحديات تتعلق بحماية البيانات والأنظمة من التهديدات السيبرانية، مما قد يؤثر سلبًا على كفاءة المشروع ونجاحه.

١,٢,١. فجوات على المستوى النظري

تتمثل الفجوة على المستوى النظري في محدودية الدراسات التي تربط بشكل مباشر بين الأمن السيبراني وإدارة المشاريع، حيث يتم تناول كل منهما بشكل منفصل دون التركيز الكافي على العلاقة التكاملية بينهما.

١,٢,٢. فجوات على المستوى التطبيقي

أما على المستوى التطبيقي، فتظهر الفجوة في ضعف تطبيق ممارسات الأمن السيبراني داخل المشاريع الرقمية، حيث تركز بعض المؤسسات على الجوانب التقليدية لإدارة المشاريع مثل الوقت والتكلفة، مع إهمال الجوانب الأمنية، مما يزيد من احتمالية التعرض للمخاطر والاختراقات و ما يترتب عليهم من آثار سلبية قد تصل إلى تعثر المشروع أو فشله.

و انطلاقًا من ذلك، تتمثل مشكلة الدراسة في الإجابة عن السؤال الرئيسي التالي :

" ما مدى تأثير الأمن السيبراني على نجاح و كفاءة إدارة المشاريع الرقمية؟ "

١,٣. أهمية الدراسة

١,٣,١. على المستوى النظري:

تتبع أهمية هذه الدراسة من مساهمتها في إثراء الأدبيات العلمية المتعلقة بإدارة المشاريع والأمن السيبراني، من خلال توضيح العلاقة بينهما وبيان دور الأمن السيبراني كعامل مؤثر في نجاح المشاريع الرقمية. كما تسعى الدراسة إلى سد الفجوة المعرفية من خلال تقديم إطار نظري يربط بين مفاهيم إدارة المشاريع وممارسات الأمن السيبراني.

١,٣,٢. على المستوى التطبيقي:

تتمثل الأهمية التطبيقية لهذه الدراسة في تقديم نتائج وتوصيات عملية تساعد مديري المشاريع والمؤسسات على تعزيز ممارسات الأمن السيبراني ضمن مشاريعهم، بما يساهم في تقليل المخاطر وحماية البيانات وتحسين كفاءة الأداء. كما تساعد الدراسة في توجيه صناع القرار إلى أهمية دمج الجوانب الأمنية في مختلف مراحل إدارة المشروع لضمان نجاحه واستمراريته.

١,٤. أسئلة الدراسة

- ما أثر الأمن السيبراني على نجاح وكفاءة إدارة المشاريع الرقمية؟
- ما مستوى تطبيق ممارسات الأمن السيبراني في المشاريع الرقمية؟
- ما دور الأمن السيبراني في تقليل المخاطر التي تواجه المشاريع الرقمية؟
- هل يؤدي ضعف الأمن السيبراني إلى تأخير أو فشل المشاريع الرقمية؟
- ما العلاقة بين مستوى الحماية السيبرانية و تقليل المخاطر في المشاريع الرقمية؟

١,٥ . أهداف الدراسة

١. التعرف على أثر الأمن السيبراني على نجاح وكفاءة إدارة المشاريع الرقمية.
٢. تحديد مستوى تطبيق ممارسات الأمن السيبراني في المشاريع الرقمية.
٣. توضيح دور الأمن السيبراني في تقليل المخاطر التي تواجه المشاريع الرقمية.
٤. تحليل تأثير ضعف الأمن السيبراني على تأخير أو فشل المشاريع الرقمية.
٥. بيان العلاقة بين مستوى تطبيق الأمن السيبراني ونجاح المشاريع الرقمية.

١,٦ . فرضيات الدراسة

المتغير المستقل (الأمن السيبراني)

المتغيرات التابعة (نجاح المشاريع الرقمية – كفاءة إدارة المشاريع – تقليل المخاطر – فشل | تأخير المشاريع)
(الفرضيات)

١. توجد علاقة ذات دلالة إحصائية بين مستوى تطبيق ممارسات الأمن السيبراني ونجاح المشاريع الرقمية.

٢. توجد علاقة ذات دلالة إحصائية بين مستوى تطبيق الأمن السيبراني وكفاءة إدارة المشاريع الرقمية.

٣. توجد علاقة ذات دلالة إحصائية بين مستوى تطبيق الأمن السيبراني وتقليل المخاطر في المشاريع الرقمية.

٤. توجد علاقة ذات دلالة إحصائية بين ضعف الأمن السيبراني وزيادة احتمالية تأخير أو فشل المشاريع الرقمية.

١,٧. نموذج الدراسة

يعتمد هذا البحث على نموذج مفاهيمي يوضح العلاقة بين *الأمن السيبراني* كمتغير مستقل، و*نجاح وكفاءة إدارة المشاريع الرقمية* كمتغيرات تابعة، بالإضافة إلى دوره في *تقليل المخاطر* وتأثيره على *تأخير أو فشل المشاريع*.

ويفترض النموذج أن مستوى تطبيق ممارسات الأمن السيبراني يؤثر بشكل مباشر على نجاح المشاريع الرقمية وكفاءة إدارتها، كما يساهم في تقليل المخاطر التي قد تواجه هذه المشاريع. وفي المقابل، فإن ضعف الأمن السيبراني قد يؤدي إلى زيادة احتمالية تأخير المشاريع أو فشلها.

ويستخدم هذا النموذج لتوجيه منهجية البحث وتحليل البيانات، من خلال اختبار العلاقات بين المتغير المستقل والمتغيرات التابعة باستخدام الأساليب الإحصائية المناسبة. يتكون نموذج البحث من العناصر التالية:

*المتغير المستقل:

مستوى تطبيق ممارسات الأمن السيبراني

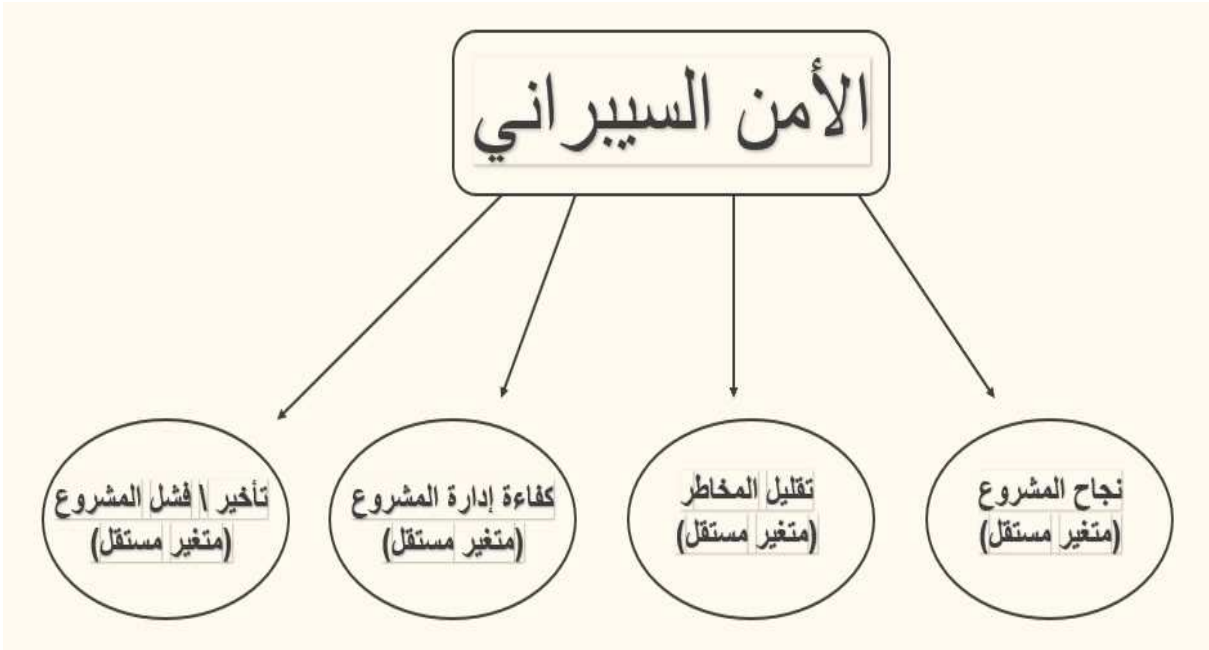
*المتغيرات التابعة:

* نجاح المشاريع الرقمية

* كفاءة إدارة المشاريع الرقمية

* تقليل المخاطر

* تأخير أو فشل المشاريع



١,٨ . منهجية الدراسة

تعتمد هذه الدراسة على المنهج الوصفي التحليلي، والذي يُعد من أكثر المناهج ملائمةً لدراسة الظواهر الإدارية وتحليل العلاقات بين المتغيرات، حيث يهدف إلى وصف واقع تطبيق ممارسات الأمن السيبراني في المشاريع الرقمية، وتحليل أثرها على نجاح وكفاءة إدارة المشاريع.

تصميم البحث

يعتمد البحث على التصميم الكمي (Quantitative Research Design)، وذلك من خلال جمع بيانات رقمية قابلة للتحليل الإحصائي، بهدف اختبار فرضيات الدراسة وقياس العلاقة بين المتغير المستقل (الأمن السيبراني) والمتغيرات التابعة (نجاح المشاريع، كفاءة الإدارة، تقليل المخاطر، وتأخير أو فشل المشاريع).

مجتمع الدراسة

يتكون مجتمع الدراسة من العاملين في مجال إدارة المشاريع الرقمية وتقنية المعلومات، بما في ذلك:

- * مدراء المشاريع
- * أعضاء فرق العمل في المشاريع الرقمية
- * المختصين في الأمن السيبراني داخل المؤسسات

عينة الدراسة

تم اختيار عينة الدراسة باستخدام أسلوب العينة العشوائية البسيطة، لضمان تمثيل عادل لمجتمع الدراسة، حيث سيتم توزيع الاستبيان على عدد من الأفراد العاملين في المجال. ويمكن أن يتراوح حجم العينة بين (٥٠ - ١٥٠) مشارك، بما يتناسب مع طبيعة الدراسة وإمكانية الوصول إلى المبحوثين.

أدوات جمع البيانات

تعتمد الدراسة على الاستبيان (Questionnaire) كأداة رئيسية لجمع البيانات، حيث تم تصميمه بناءً على محاور الدراسة، ويتكون من عدة أقسام، منها:

١. البيانات الديموغرافية (مثل: العمر، الخبرة، المسمى الوظيفي)
 ٢. مستوى تطبيق ممارسات الأمن السيبراني
 ٣. مستوى نجاح المشاريع الرقمية
 ٤. كفاءة إدارة المشاريع
 ٥. تقليل المخاطر
 ٦. تأثير ضعف الأمن السيبراني على تأخير أو فشل المشاريع
- ويتم قياس الإجابات باستخدام مقياس ليكرت الخماسي (من موافق بشدة إلى غير موافق بشدة).

تقنيات تحليل البيانات

سيتم تحليل البيانات باستخدام الأساليب الإحصائية المناسبة، ومن أبرزها:

الإحصاء الوصفي: مثل المتوسطات الحسابية والانحراف المعياري، لوصف خصائص العينة

اختبار الارتباط (Correlation): لقياس العلاقة بين المتغيرات

تحليل الانحدار (Regression Analysis): لاختبار تأثير الأمن السيبراني على المتغيرات التابعة

استخدام برامج إحصائية مثل **SPSS** لتحليل البيانات واستخراج النتائج

الاعتبارات الأخلاقية

- تلتزم الدراسة بعدد من المبادئ الأخلاقية، من أهمها:
- * ضمان سرية معلومات المشاركين وعدم استخدامها إلا لأغراض البحث العلمي
 - * استخدام البيانات بشكل جماعي دون الإشارة إلى أي أسماء أو معلومات شخصية
 - * الحصول على موافقة المشاركين قبل تعبئة الاستبيان
 - * توضيح هدف الدراسة للمشاركين بشكل شفاف

١,٩ . الدراسة الميدانية

تهدف الدراسة الميدانية إلى التعرف على أثر تطبيق ممارسات الأمن السيبراني على نجاح وكفاءة إدارة المشاريع الرقمية، وذلك من خلال جمع بيانات ميدانية من عينة من العاملين في مجال إدارة المشاريع وتقنية المعلومات، وتحليلها إحصائيًا لاختبار فرضيات الدراسة.

أداة الدراسة

تم استخدام الاستبيان كأداة رئيسية لجمع البيانات، حيث تم تصميمه بناءً على أهداف الدراسة وفرضياتها، ويتكون من عدة محاور تغطي متغيرات الدراسة (الأمن السيبراني، نجاح المشاريع، كفاءة الإدارة، تقليل المخاطر، وتأخير أو فشل المشاريع).

توزيع الاستبيان

تم توزيع الاستبيان إلكترونياً عبر منصة Google Forms على عينة من العاملين في مجال إدارة المشاريع الرقمية، وتم الحصول على عدد مناسب من الاستجابات التي تم تحليلها.

صدق وثبات الأداة

تم التأكد من صدق الأداة من خلال عرضها على عدد من المختصين، كما تم التأكد من ثباتها باستخدام معامل (كرونباخ ألفا)، مما يدل على أن الأداة مناسبة للتحليل.

تحليل البيانات

تم تحليل البيانات باستخدام برنامج SPSS من خلال:

* المتوسطات الحسابية

* الانحراف المعياري

* معامل الارتباط

* تحليل الانحدار

أسئلة الاستبيان

يتكون الاستبيان من عدة محاور رئيسية، وتم استخدام مقياس ليكرت الخماسي (موافق بشدة، موافق، محايد، غير موافق، غير موافق بشدة) لقياس إجابات أفراد العينة، وذلك على النحو التالي:

♦ القسم الأول: البيانات الديموغرافية (اختياري / اختيار من متعدد)

١. الجنس:

* ذكر

* أنثى

٢. العمر:

* أقل من ٢٥

* ٢٥ – ٣٥

* ٣٦ – ٤٥

* أكثر من ٤٥

٣. سنوات الخبرة:

* أقل من سنة

* ١ – ٥ سنوات

* ٦ – ١٠ سنوات

* أكثر من ١٠ سنوات

٤. المسمى الوظيفي:

* مدير مشروع

* عضو فريق مشروع

* مختص تقنية معلومات

* مختص أمن سيبراني

♦ القسم الثاني: الأمن السيبراني (المتغير المستقل)

(مقياس ليكرت: موافق بشدة – موافق – محايد – غير موافق – غير موافق بشدة)

١. يتم تطبيق سياسات الأمن السيبراني بشكل واضح داخل المشاريع.

٢. يتم تدريب فريق العمل على أساسيات الأمن السيبراني.

٣. توجد أنظمة حماية فعالة ضد الهجمات الإلكترونية.
٤. يتم تحديث أنظمة الحماية بشكل دوري.
٥. يتم التعامل مع المخاطر الأمنية بشكل سريع وفعال.

◆ القسم الثالث: نجاح المشاريع الرقمية

١. تحقق المشاريع الرقمية أهدافها بنجاح.
٢. يتم تسليم المشاريع في الوقت المحدد.
٣. يتم الالتزام بميزانية المشروع.
٤. جودة مخرجات المشاريع الرقمية مرتفعة.

◆ القسم الرابع: كفاءة إدارة المشاريع

١. يتم إدارة الموارد بكفاءة داخل المشروع.
٢. يتم اتخاذ القرارات بسرعة وفعالية.
٣. توجد متابعة مستمرة لسير العمل.
٤. يتم حل المشكلات بشكل احترافي.

◆ القسم الخامس: تقليل المخاطر

١. يساهم الأمن السيبراني في تقليل المخاطر في المشاريع.
٢. يتم تحديد المخاطر الأمنية قبل حدوثها.
٣. توجد خطط واضحة لإدارة المخاطر.
٤. يقل حدوث الأعطال بسبب تطبيق الأمن السيبراني.

◆ القسم السادس: تأخير أو فشل المشاريع

١. ضعف الأمن السيبراني يؤدي إلى تأخير المشاريع.
٢. الهجمات الإلكترونية تؤثر على سير العمل.
٣. نقص الحماية قد يؤدي إلى فشل المشروع.
٤. تسريب البيانات يؤثر سلبًا على المشروع.

١,١٠. مخطط المشروع المقترح

يهدف المشروع المقترح إلى دراسة أثر الأمن السيبراني على نجاح وكفاءة إدارة المشاريع الرقمية، وذلك من خلال تنفيذ مجموعة من المراحل المنظمة وفق منهجية إدارة المشاريع. ويتكون مخطط المشروع من العناصر التالية:

١. تعريف المشروع

مشروع بحثي يركز على تحليل دور الأمن السيبراني في تحسين أداء المشاريع الرقمية وتقليل المخاطر المرتبطة بها.

٢. أهداف المشروع

- * دراسة أثر الأمن السيبراني على نجاح المشاريع الرقمية
- * تحليل دوره في تحسين كفاءة إدارة المشاريع
- * تقييم تأثيره في تقليل المخاطر
- * التعرف على العلاقة بين ضعف الأمن السيبراني وفشل المشاريع

٣. نطاق المشروع (Project Scope)

يشمل المشروع:

- * المشاريع الرقمية داخل المؤسسات
 - * ممارسات الأمن السيبراني المرتبطة بها
 - * تحليل العلاقة بين الأمن السيبراني وأداء المشاريع
- ولا يشمل:
- * الجوانب التقنية التفصيلية العميقة للأمن السيبراني
 - * مشاريع غير رقمية

٤. مخرجات المشروع (Deliverables)

- * إعداد استبيان
- * جمع وتحليل البيانات
- * تقرير بحثي نهائي
- * نتائج وتوصيات عملية

٥. الجدول الزمني للمشروع (Timeline)

يمكن تقسيم المشروع إلى مراحل:

١. إعداد الإطار النظري
٢. تصميم أداة الدراسة (الاستبيان)

- ٣. جمع البيانات
- ٤. تحليل البيانات
- ٥. كتابة النتائج والتوصيات

- ٦. الموارد المطلوبة
 - * جهاز حاسب آلي
 - * برنامج SPSS
 - * منصة Google Forms
 - * مراجع علمية

- ٧. إدارة المخاطر
 - من أبرز المخاطر:
 - * ضعف استجابة المشاركين
 - * عدم دقة البيانات
 - * ضيق الوقت
 - طرق التعامل:
 - * توزيع الاستبيان على عدد أكبر
 - * تبسيط الأسئلة
 - * تنظيم الوقت

- ٨. معايير نجاح المشروع
 - * الحصول على بيانات كافية للتحليل
 - * تحقيق أهداف الدراسة
 - * الوصول إلى نتائج واضحة تدعم الفرضيات
 - * تقديم توصيات قابلة للتطبيق

٢. الفصل الثاني: الدراسات السابقة

٢,١ . المقدمة:

٢,٢ . المتغير المستقل

٢,٣ . المتغير التابع

٢,٤ . العلاقة بين المتغير المستقل والمتغير التابع

٢,٥ . الخاتمة

- Kerzner, H. (2017). Project Management: A Systems Approach .to Planning, Scheduling, and Controlling. John Wiley & Sons
- Project Management Institute. (2021). A Guide to the Project .Management Body of Knowledge (PMBOK Guide) (7th ed.)
- Stallings, W. (2017). Effective Cybersecurity: A Guide to Using .Best Practices and Standards. Addison-Wesley
- Whitman, M. E., & Mattord, H. J. (2018). Principles of .Information Security. Cengage Learning
- ISO. (2018). ISO/IEC 27001 Information Security Management .Systems
- NIST. (2020). Cybersecurity Framework. National Institute of .Standards and Technology