

جامعة ميدأوشن



كلية الإدارة

قسم / تخصص. ماجستير إدارة الأعمال

عنوان البحث

أثر الأمن السيبراني على فعالية إدارة المشاريع التقنية: دراسة تطبيقية على القطاع

الحكومي في المملكة العربية السعودية

إعداد الطالب/منصور دغفق العنزي

إشراف/

د. الفیصل عبدالحمید محمد

د. فايز علي جراد

العام الدراسي:

202٥

## جدول المحتويات

|    |                                     |
|----|-------------------------------------|
| ٥  | الفصل الأول                         |
| ٦  | الملخص                              |
| ٧  | مقدمة الدراسة                       |
| ٩  | مشكلة الدراسة                       |
| ١٠ | أهمية الدراسة                       |
| ١٢ | أهداف الدراسة                       |
| ١٤ | تساؤلات الدراسة                     |
| ١٦ | فرضيات الدراسة                      |
| ١٧ | مصطلحات الدراسة                     |
| ١٨ | متغيرات الدراسة                     |
| ١٩ | الفصل الثاني                        |
| ٢٠ | الدراسات السابقة                    |
| ٢٥ | الإطار النظري                       |
| ٣٠ | مفهوم وأهمية إدارة المشاريع التقنية |

|    |                                                                       |
|----|-----------------------------------------------------------------------|
| ٣٤ | الأمن السيبراني: المفاهيم الأساسية والتهديدات                         |
| ٣٨ | العلاقة بين الأمن السيبراني وإدارة المشاريع                           |
| ٤٢ | الإطار التنظيمي والتشريعي للأمن السيبراني في المملكة العربية السعودية |
| ٤٧ | تكامل الأمن السيبراني في مراحل دورة حياة المشروع                      |
| ٥١ | معايير وأطر الأمن السيبراني المطبقة في القطاع الحكومي                 |
| ٥٤ | تحديات الأمن السيبراني في سياق المشاريع التقنية الحكومية              |
| ٥٧ | دور العنصر البشري في الأمن السيبراني للمشاريع                         |
| ٥٨ | أفضل الممارسات لتعزيز الأمن السيبراني في إدارة المشاريع               |
| ٥٩ | الخاتمة                                                               |
| ٦٠ | الفصل الثالث                                                          |
| ٦١ | منهجية الدراسة                                                        |
| ٦١ | مجتمع الدراسة                                                         |
| ٦٢ | أدوات جمع البيانات                                                    |
| ٦٣ | حدود الدراسة                                                          |

|    |                  |
|----|------------------|
| ٦٤ | الاستبيان        |
| ٧٠ | الفصل الرابع     |
| ٧١ | التحليل الإحصائي |
| ٨٦ | النتائج          |
| ٨٩ | التوصيات         |
| ٩٢ | المراجع          |
| ٩٥ | الملخص           |
| ٩٦ | الملاحق          |

## ملخص الدراسة

هدفت هذه الدراسة إلى تحديد وتحليل أثر الأمن السيبراني على فعالية إدارة المشاريع

التقنية في القطاع الحكومي بالمملكة العربية السعودية. جاءت هذه الأهمية في ظل

التوسع الرقمي الذي تشهده المملكة ورؤية 2030، والتي تضع الأمن السيبراني كركيزة

أساسية لنجاح المشاريع التقنية الحكومية.

تضمنت مشكلة الدراسة الرئيسية سؤالاً حول مدى تأثير الأمن السيبراني على فعالية إدارة

المشاريع، وتفرعت منها أسئلة حول تكامل الأمن السيبراني، تأثيره على مؤشرات الأداء

(الوقت، التكلفة، الجودة)، أبرز التحديات الأمنية، ومستوى الوعي والتدريب.

لتحقيق أهدافها، اعتمدت الدراسة على المنهج الوصفي التحليلي، وتم استخدام الاستبانة

كأداة رئيسية لجمع البيانات من مجتمع الدراسة المتمثل في العاملين بإدارة المشاريع التقنية

والأمن السيبراني في القطاع الحكومي السعودي. تم تحليل 100 استجابة باستخدام

الإحصاء الوصفي.

أظهرت النتائج أن هناك وعياً جيداً بأهمية دمج الأمن السيبراني في تخطيط المشاريع،

وأن الالتزام بمعايير الأمن السيبراني يؤثر إيجاباً على جودة مخرجات المشاريع. ومع ذلك،

كشفت النتائج عن فجوة في التكامل المستمر للأمن السيبراني خلال مراحل المشروع، وأن

التحديات الأمنية السيبرانية (حتى لو لم تكن متكررة) تؤدي إلى تأخيرات وزيادات في

التكلفة وتأثير سلبي على جودة المشاريع. كما أشارت النتائج إلى الحاجة لتعزيز برامج التدريب على الأمن السيبراني لفرق عمل المشاريع.

بناءً على هذه النتائج، أوصت الدراسة بتعزيز التكامل الشامل للأمن السيبراني في جميع مراحل دورة حياة المشروع، والموازنة بين متطلبات الأمن وقيود المشروع (الوقت والتكلفة)، والاستثمار في برامج التدريب المتخصصة ورفع الكفاءة، وتطوير آليات استباقية لإدارة التحديات الأمنية، وأخيرًا تفعيل دور قيادات الأمن السيبراني في صنع القرار، بهدف تحقيق مشاريع تقنية أكثر فعالية وأمانًا في القطاع الحكومي بالمملكة.

شهدت المملكة العربية السعودية في السنوات الأخيرة تحولاً رقمياً غير مسبوق، مدفوعاً برؤية 2030 الطموحة، التي تهدف إلى بناء اقتصاد مزدهر ومجتمع حيوي وحكومة فاعلة. يُعد القطاع الحكومي ركيزة أساسية في تحقيق هذه الرؤية، حيث تتزايد وتيرة تبني التقنيات الحديثة وتنفيذ المشاريع التقنية المعقدة لتقديم خدمات أفضل للمواطنين والمقيمين. ومع هذا التوسع في الاعتماد على البنية التحتية الرقمية والأنظمة المتصلة بالإنترنت، يبرز تحدٍ محوري يتمثل في الأمن السيبراني. لم يعد الأمن السيبراني مجرد قضية تقنية بحتة، بل أصبح عاملاً حاسماً يؤثر بشكل مباشر على فعالية ونجاح إدارة المشاريع التقنية، لا سيما في بيئة حساسة وحيوية كالقطاع الحكومي. ففي ظل التهديدات السيبرانية المتزايدة والمتطورة، من هجمات الفدية والتصيد الاحتيالي إلى اختراقات البيانات والتجسس السيبراني، أصبحت القدرة على حماية الأصول الرقمية وضمان استمرارية الأعمال أولوية قصوى. تهدف هذه الدراسة إلى استكشاف العلاقة بين الأمن السيبراني وفعالية إدارة المشاريع التقنية في القطاع الحكومي بالمملكة العربية السعودية، وتحليل كيفية تأثير تدابير الأمن السيبراني المطبقة على تحقيق أهداف المشاريع ضمن الجدول الزمني والميزانية المحددين وبالمعايير المطلوبة.

على الرغم من الاستثمارات الضخمة في البنية التحتية التقنية وتبني أفضل الممارسات في إدارة المشاريع، لا تزال المشاريع التقنية في القطاع الحكومي بالمملكة العربية السعودية تواجه تحديات كبيرة قد تؤثر على فعاليتها، ومن أبرز هذه التحديات تلك المتعلقة بضعف الأمن السيبراني أو عدم كفاية تدابيرته. إن عدم إيلاء الأمن السيبراني الأهمية الكافية منذ مراحل التخطيط الأولية للمشاريع، أو عدم تكامله بشكل فعال في دورة حياة المشروع، يمكن أن يؤدي إلى عواقب وخيمة تشمل تأخيرات في الجدول الزمني، تجاوز الميزانية، انخفاض جودة المخرجات، وفي أسوأ الأحوال، فشل المشروع بالكامل بسبب الاختراقات الأمنية أو فقدان البيانات الحساسة.

#### المشكلة الرئيسية:

ما هو أثر الأمن السيبراني على فعالية إدارة المشاريع التقنية في القطاع الحكومي بالمملكة العربية السعودية؟

#### المشكلات الفرعية:

1. ما مدى تكامل مبادئ ومعايير الأمن السيبراني في مراحل تخطيط وتنفيذ المشاريع

التقنية بالقطاع الحكومي؟

2. كيف يؤثر الالتزام بمعايير الأمن السيبراني (مثل CIS، ISO 27001،

Controls) على مؤشرات أداء المشاريع التقنية (الوقت، التكلفة، الجودة)؟

3. ما هي أبرز التحديات الأمنية السيبرانية التي تواجه المشاريع التقنية في القطاع

الحكومي، وكيف تؤثر على فعاليتها؟

4. ما هو مستوى الوعي والتدريب الخاص بالأمن السيبراني لدى فرق عمل المشاريع

التقنية في القطاع الحكومي؟

5. ما هي أفضل الممارسات المقترحة لتعزيز الأمن السيبراني في إدارة المشاريع

التقنية لزيادة فعاليتها في القطاع الحكومي؟

الأهمية العلمية والعملية للدراسة

تكتسب هذه الدراسة أهمية بالغة على الصعيدين العلمي والعملية، وذلك للأسباب التالية:

الأهمية العلمية:

1. سد فجوة بحثية: تسهم الدراسة في سد فجوة بحثية واضحة في الأدبيات العربية

والدراسات التطبيقية التي تربط بشكل مباشر بين الأمن السيبراني وفعالية إدارة

المشاريع التقنية، خاصة في سياق القطاع الحكومي بالمملكة العربية السعودية،

والذي يتميز بخصائص تنظيمية وتشريعية فريدة.

2. تطوير الإطار النظري: تعمل الدراسة على إثراء الإطار النظري المتعلق بإدارة

المشاريع والأمن السيبراني من خلال تقديم نموذج تحليلي يوضح العلاقة السببية

بين المتغيرات، مما يمكن أن يكون أساسًا لدراسات مستقبلية.

3. توفير بيانات تحليلية: تقدم الدراسة بيانات وتحليلات معمقة حول تأثير التحديات

والتدابير الأمنية السيبرانية على أداء المشاريع، مما يدعم الباحثين والأكاديميين في

فهم أعمق لهذا المجال المتطور.

4. منهجية متعددة الأبعاد: تعتمد الدراسة على منهجية بحثية شاملة قد تشمل الجوانب

الكمية والنوعية، مما يوفر رؤى متكاملة ويضيف قيمة علمية للمنهجيات البحثية

في هذا المجال.

الأهمية العملية:

1. دعم اتخاذ القرار: توفر الدراسة نتائج وتوصيات عملية يمكن للمسؤولين وصناع

القرار في القطاع الحكومي السعودي الاستفادة منها في تطوير استراتيجيات

وسياسات فعالة لتعزيز الأمن السيبراني في المشاريع التقنية، وبالتالي تحسين

فعاليتها.

2. تحسين أداء المشاريع: من خلال تحديد أبرز التحديات وتقديم أفضل الممارسات،

يمكن للمؤسسات الحكومية تحسين قدرتها على تسليم المشاريع التقنية في الوقت

المحدد، ضمن الميزانية، وبجودة عالية، مع تقليل المخاطر الأمنية.

3. رفع الوعي: تساهم الدراسة في زيادة الوعي بأهمية الأمن السيبراني كعنصر أساسي لنجاح المشاريع التقنية، ليس فقط بين مديري المشاريع والفرق التقنية، بل بين جميع أصحاب المصلحة المعنيين.
4. توجيه التدريب والتطوير: يمكن أن تستفيد منها الجهات المعنية في تصميم برامج تدريب وتطوير مستهدفة لرفع كفاءة العاملين في مجال الأمن السيبراني وإدارة المشاريع، بما يتماشى مع التهديدات والتقنيات الحديثة.
5. المساهمة في تحقيق رؤية 2030: تدعم الدراسة بشكل مباشر أهداف رؤية المملكة 2030 من خلال المساهمة في بناء قطاع حكومي رقمي آمن وفعال، قادر على تقديم خدمات إلكترونية موثوقة ومحمية.

## أهداف الدراسة

تهدف هذه الدراسة بشكل رئيسي إلى تحديد وتحليل أثر الأمن السيبراني على فعالية إدارة المشاريع التقنية في القطاع الحكومي بالمملكة العربية السعودية. وينبثق من هذا الهدف الرئيسي الأهداف الفرعية التالية:

- الهدف الرئيسي: تحديد وتحليل أثر الأمن السيبراني على فعالية إدارة المشاريع التقنية في القطاع الحكومي بالمملكة العربية السعودية.
- الأهداف الفرعية:

1. تحديد مدى تكامل مبادئ ومعايير الأمن السيبراني في مراحل تخطيط وتنفيذ المشاريع التقنية بالقطاع الحكومي.
2. تقييم كيفية تأثير الالتزام بمعايير الأمن السيبراني (مثل ISO 27001، CIS Controls) على مؤشرات أداء المشاريع التقنية (الوقت، التكلفة، الجودة).
3. الكشف عن أبرز التحديات الأمنية السيبرانية التي تواجه المشاريع التقنية في القطاع الحكومي، وكيف تؤثر على فعاليتها.
4. قياس مستوى الوعي والتدريب الخاص بالأمن السيبراني لدى فرق عمل المشاريع التقنية في القطاع الحكومي.

5. اقتراح أفضل الممارسات لتعزيز الأمن السيبراني في إدارة المشاريع التقنية  
لزيادة فعاليتها في القطاع الحكومي.

#### تساؤلات الدراسة

تعتبر تساؤلات الدراسة بمثابة المحاور التي تسعى الدراسة للإجابة عليها، وتوجه مسار  
البحث وجمع البيانات وتحليلها.

#### • التساؤل الرئيسي:

ما هو أثر الأمن السيبراني على فعالية إدارة المشاريع التقنية في القطاع الحكومي  
بالمملكة العربية السعودية؟

#### • التساؤلات الفرعية:

1. ما مدى تكامل مبادئ ومعايير الأمن السيبراني في مراحل تخطيط وتنفيذ

المشاريع التقنية بالقطاع الحكومي؟

2. كيف يؤثر الالتزام بمعايير الأمن السيبراني على مؤشرات أداء المشاريع

التقنية (الوقت، التكلفة، الجودة) في القطاع الحكومي؟

3. ما هي أبرز التحديات الأمنية السيبرانية التي تواجه المشاريع التقنية في

القطاع الحكومي، وكيف تؤثر على فعاليتها؟

4. ما هو مستوى الوعي والتدريب الخاص بالأمن السيبراني لدى فرق عمل

المشاريع التقنية في القطاع الحكومي؟

5. ما هي أفضل الممارسات المقترحة لتعزيز الأمن السيبراني في إدارة

المشاريع التقنية لزيادة فعاليتها في القطاع الحكومي؟

فرضيات الدراسة

تعد فرضيات الدراسة عبارات قابلة للاختبار تفترض وجود علاقة بين متغيرين أو أكثر.

ستقوم الدراسة باختبار صحة هذه الفرضيات بناءً على البيانات التي سيتم جمعها

وتحليلها.

• الفرضية الرئيسية:

يوجد أثر ذو دلالة إحصائية للأمن السيبراني على فعالية إدارة المشاريع التقنية في

القطاع الحكومي بالمملكة العربية السعودية.

• الفرضيات الفرعية:

1. يوجد تكامل فعال لمبادئ ومعايير الأمن السيبراني في مراحل تخطيط

وتنفيذ المشاريع التقنية بالقطاع الحكومي.

2. يؤثر الالتزام بمعايير الأمن السيبراني بشكل إيجابي على مؤشرات أداء

المشاريع التقنية (الوقت، التكلفة، الجودة) في القطاع الحكومي.

3. تؤثر التحديات الأمنية السيبرانية بشكل سلبي على فعالية إدارة المشاريع

التقنية في القطاع الحكومي.

4. يوجد مستوى مرتفع من الوعي والتدريب الخاص بالأمن السيبراني لدى فرق

عمل المشاريع التقنية في القطاع الحكومي.

5. يمكن لتبني أفضل الممارسات المقترحة لتعزيز الأمن السيبراني أن يساهم

في زيادة فعالية إدارة المشاريع التقنية في القطاع الحكومي.

#### مصطلحات الدراسة

لتوضيح المفاهيم الأساسية المستخدمة في هذه الدراسة، سيتم تعريف المصطلحات التالية:

- الأمن السيبراني (Cybersecurity): يُعرف بأنه مجموع الأدوات والعمليات والممارسات المصممة لحماية الشبكات والأجهزة والبرامج والبيانات من الهجمات أو التلف أو الوصول غير المصرح به. يشمل ذلك حماية سرية وسلامة وتوافر المعلومات والأنظمة.
- إدارة المشاريع التقنية (Technical Project Management): هي عملية تخطيط وتنظيم وتحفيز ومراقبة الموارد لتحقيق أهداف محددة للمشاريع التي

تتضمن مكونات تقنية كبيرة، مثل تطوير البرمجيات، نشر البنية التحتية، أو تنفيذ الأنظمة الرقمية. تتضمن الالتزام بالوقت والميزانية والجودة.

- فعالية إدارة المشاريع (Project Management Effectiveness): تُقاس

فعالية إدارة المشاريع بقدرة المشروع على تحقيق أهدافه المحددة ضمن القيود

الثلاثية: الوقت، التكلفة، والجودة. كما تشمل رضا أصحاب المصلحة والمخرجات التي تلبي المتطلبات المحددة.

- القطاع الحكومي (Government Sector): يشير إلى الهيئات والوزارات

والمؤسسات الحكومية على المستويات المختلفة التي تقدم الخدمات العامة وتنفذ السياسات في المملكة العربية السعودية.

- معايير الأمن السيبراني (Cybersecurity Standards): هي مجموعة من

الإرشادات والمواصفات والمتطلبات التي تهدف إلى توفير إطار عمل لتعزيز الأمن السيبراني. من أمثلتها:

- ISO/IEC 27001: معيار دولي لنظام إدارة أمن المعلومات (ISMS).

- CIS Controls: مجموعة من الإجراءات الأمنية التي يمكن للمؤسسات

اتخاذها لتعزيز دفاعاتها السيبرانية.

- التحديات الأمنية السيبرانية (Cybersecurity Challenges): هي العقبات

والمخاطر التي تواجه الأنظمة والبيانات بسبب التهديدات السيبرانية، مثل هجمات

الفدية، التصيد الاحتيالي، البرمجيات الخبيثة، اختراق البيانات، والتجسس  
السيبراني.

- مؤشرات أداء المشاريع (Project Performance Indicators – KPIs): هي مقاييس قابلة للقياس تستخدم لتقييم مدى نجاح المشروع في تحقيق أهدافه. في هذه الدراسة، تشمل:

- الوقت (Time): مدى الالتزام بالجدول الزمني المحدد للمشروع.
- التكلفة (Cost): مدى الالتزام بالميزانية المخصصة للمشروع.
- الجودة (Quality): مدى مطابقة مخرجات المشروع للمواصفات والمتطلبات المحددة.

#### متغيرات الدراسة

لتحديد العلاقات بين المفاهيم التي تتناولها الدراسة، يتم تحديد المتغيرات كالتالي:

- المتغير المستقل (Independent Variable):
    - الأمن السيبراني: ويمثل المفهوم الذي يتم دراسة تأثيره على المتغير التابع.
- يشمل ذلك:

- تكامل مبادئ ومعايير الأمن السيبراني في مراحل المشروع.

▪ الالتزام بمعايير الأمن السيبراني (مثل CIS ، ISO 27001

.(Controls

▪ التحديات الأمنية السيبرانية (كمؤشر عكسي لتطبيق الأمن السيبراني

الفعال).

▪ مستوى الوعي والتدريب الخاص بالأمن السيبراني.

• المتغير التابع (Dependent Variable):

○ فعالية إدارة المشاريع التقنية: ويمثل المفهوم الذي يتأثر بالمتغير المستقل.

تُقاس الفعالية من خلال مؤشرات الأداء التالية:

▪ الوقت: مدى تحقيق المشروع للجدول الزمني المحدد.

▪ التكلفة: مدى التزام المشروع بالميزانية المخصصة.

▪ الجودة: مدى مطابقة مخرجات المشروع للمعايير والمتطلبات

المحددة.

## الفصل الثاني

## الدراسات السابقة

### (1) دراسة الحبيب (2022)

عنوان الدراسة: درجة الوعي بالأمن السيبراني لدى طلاب وطالبات الدراسات العليا بكلية التربية بجامعة الإمام محمد بن سعود الإسلامية وسبل تعزيزه من وجهة نظرهم.

المؤلف: الحبيب

النتائج:

- درجة الوعي بالأمن السيبراني لدى الطلاب والطالبات كانت عالية.
  - درجة الوعي بتطبيقات الأمن السيبراني كانت عالية.
  - أبرز سبل تعزيز الوعي بالأمن السيبراني كانت عالية.
- أوصت الدراسة: بتنظيم دورات عن الأمن السيبراني في كل فصل دراسي وعدم ربط أجهزة الطلاب والطالبات بأجهزة العرض في القاعات الدراسية دون إحضار ما يثبت حضورهم الدورة في الأمن السيبراني، وخلو أجهزتهم من الفيروسات.

### (2) دراسة الحداد (2022)

عنوان الدراسة: متطلبات تحقيق الأمن السيبراني في المكتبات الجامعية اليمنية دراسة حالة.

المؤلف: الحداد

## النتائج:

- المتطلبات المادية والتقنية لتحقيق الأمن السيبراني في المكتبات الجامعية اليمنية كانت في المرتبة الأولى.
- المتطلبات البشرية والمالية كانت في المرتبة الثانية.
- المكتبات اليمنية تفتقر إلى متطلبات تحقيق الأمن السيبراني بسبب ضعف الموارد المالية وغياب الكوادر البشرية المؤهلة في مجال الأمن السيبراني، وضعف التقنية.
- أوصت الدراسة: بتوفير كوادر بشرية خاصة بالأمن السيبراني في الجامعات اليمنية وتوفير الدعم المالي لتحقيق الأمن السيبراني وحفظ البيانات من قبل الجامعات اليمنية.

## (3) دراسة فرج (2022)

عنوان الدراسة: دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي - جامعة الأمير سطاتم بن عبد العزيز نموذجًا.

المؤلف: فرج

## النتائج:

- دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي بجامعة الأمير سطاتم بن عبد العزيز من وجهة نظر أعضاء هيئة التدريس حصلت على متوسط عام (3.55) من (5)، وهي درجة متوسطة.

- محور الدواعي المجتمعية لتعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي بالجامعة حصل على أعلى متوسط (3.70).

- محور الدواعي المعرفية لتعزيز ثقافة الأمن السيبرانية بالجامعة حصل على متوسط (3.51) عام.

- محور الدواعي التقنية حصل على متوسط (3.46).

- عدم وجود فروق ذات دلالة إحصائية تبعًا لمتغير الكلية، والرتبة العلمية.

- وجود فروق تعزى لمتغير سنوات الخبرة.

توصي الدراسة: بأهمية إنكاء الوعي بالأمن السيبراني لدى الطلبة، وإدراك منافع البرمجيات المتاحة لمكافحة المخاطر السيبرانية، وتصميم حملات للتوعية بالمخاطر السيبرانية.

(4) دراسة زقوت (2022)

عنوان الدراسة: مدى وعي أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبراني في ظل التحول الرقمي - دراسة تطبيقية بجامعة الزاوية.

المؤلف: زقوت

النتائج:

- وجود علاقة ذات دلالة إحصائية حول وعي أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبراني في ظل التحول الرقمي في محل الدراسة (جامعة الزاوية).

توصيات الدراسة:

- عقد دورات تدريبية لأعضاء هيئة التدريس تركز على الأمن السيبراني.
- إدراج مجال الأمن السيبراني ضمن مناهج التعليم في المدارس والجامعات.
- تشجيع بحوث ودراسات الأمن السيبراني في دراسات الماجستير والدكتوراه.
- إجراء دراسات حول مخاطر الجرائم السيبرانية.

دراسة الجنفاوي (2021)

عنوان الدراسة: التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت.

المؤلف: الجنفاوي

النتائج:

- مستوى تطبيق المؤسسات الوطنية للتحول الرقمي وإدارة الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت كان متوسطاً.

- عدم وجود فروق ذات دلالة إحصائية حول التحول الرقمي وإدارة الأمن السيبراني راجعة لمتغيرات العمر والمؤهل العلمي والخبرات العملية، والدورات التدريبية.

توصيات الدراسة:

- ضرورة استقطاب خبرات متخصصة ومحترفة في المؤسسات الوطنية بدولة الكويت.
- زيادة التعاون والتنسيق مع المنظمات المحلية والإقليمية والدولية فيما يتعلق بإدارة الأمن السيبراني.

(6) دراسة Wangen (2021) & Ulven

عنوان الدراسة: مراجعة منهجية لمخاطر الأمن السيبراني في التعليم العالي.

المؤلف: Wangen & Ulven

النتائج:

- الأبحاث التجريبية في مجال مخاطر الأمن السيبراني نادرة.
- وجود فجوة كبيرة في نتائج الدراسات والبحوث التي تمت مراجعتها على فترة زمنية تجاوزت (12) عامًا.

- وجود اتفاق كبير حول متطلبات ومصادر الأمن السيبراني، وأهمية الأمن السيبراني في حماية وأمن المعلومات.

- وجود تسع مخاطر إلكترونية حقيقية تحتاج إلى أمن سيبراني.

## (7) دراسة السمحان (2020)

عنوان الدراسة: متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود.

المؤلف: السمحان

النتائج:

- اعتمدت الدراسة على الاستبانة كأداة لجمع المعلومات من عينة من العاملين بجامعة الملك سعود بالرياض.
- هدفت الدراسة إلى معرفة وجهة نظر العاملين حول كيفية تحقيق الأمن السيبراني بالجامعة من خلال المتطلبات الإدارية والتقنية والبشرية.

## الإطار النظري

### المحور الأول: مفهوم وأهمية إدارة المشاريع التقنية

- مفهوم إدارة المشاريع: تعريف إدارة المشاريع، مراحل دورة حياة المشروع (البدء، التخطيط، التنفيذ، المراقبة والتحكم، الإغلاق).
- المشاريع التقنية: خصائص المشاريع التقنية، تحدياتها، وأهميتها في تحقيق أهداف المؤسسات.
- فعالية إدارة المشاريع: معايير قياس فعالية المشروع (الالتزام بالوقت، الميزانية، الجودة)، رضا أصحاب المصلحة، تحقيق أهداف الأعمال.

### المحور الثاني: الأمن السيبراني: المفاهيم الأساسية والتهديدات

- تعريف الأمن السيبراني: المبادئ الأساسية (السرية، السلامة، التوافر)، الفرق بين أمن المعلومات والأمن السيبراني.
- أهمية الأمن السيبراني: في البيئة الرقمية الحديثة، الأثر على الثقة، سمعة المؤسسات، واستمرارية الأعمال.
- أنواع التهديدات السيبرانية: البرمجيات الخبيثة (الفدية، الفيروسات)، التصيد الاحتيالي، هجمات حجب الخدمة الموزعة (DDoS)، اختراقات البيانات، التجسس السيبراني، الهجمات المتقدمة المستمرة (APT).

- أثر التهديدات على المشاريع التقنية: المخاطر المباشرة وغير المباشرة على المشاريع.

#### المحور الثالث: العلاقة بين الأمن السيبراني وإدارة المشاريع

- الأمن السيبراني كجزء لا يتجزأ من إدارة المشاريع: التحول من كونه "إضافة" إلى "عنصر أساسي".
- تأثير مخاطر الأمن السيبراني على خطط المشروع: الجدولة، الميزانية، نطاق العمل، إدارة المخاطر، إدارة الجودة.
- الأمن السيبراني كعامل تمكين: كيف يمكن للأمن السيبراني القوي أن يدعم نجاح المشاريع التقنية.

#### المحور الرابع: الإطار التنظيمي والتشريعي للأمن السيبراني في المملكة العربية السعودية

- الهيئة الوطنية للأمن السيبراني (NCA): دورها، استراتيجيتها، وأهدافها في تعزيز الأمن السيبراني على المستوى الوطني.
- اللوائح والسياسات الوطنية: استعراض لأهم اللوائح والإرشادات الصادرة عن الهيئة الوطنية للأمن السيبراني أو جهات أخرى ذات صلة بالقطاع الحكومي.
- رؤية 2030 والأمن السيبراني: كيف تدعم الرؤية بناء قطاع رقمي آمن ومرن.

## المحور الخامس: تكامل الأمن السيبراني في مراحل دورة حياة المشروع

- الأمن في مرحلة البدء والتخطيط: تحديد المتطلبات الأمنية، تحليل المخاطر الأولية، الموازنة بين الأهداف الأمنية وأهداف المشروع.
- الأمن في مرحلة التنفيذ: التطوير الآمن ( Secure Development Life Cycle – SDLC)، الاختبار الأمني، إدارة الثغرات.
- الأمن في مرحلة المراقبة والإغلاق: المراقبة الأمنية المستمرة، إدارة الحوادث، التوثيق، الدروس المستفادة.

## المحور السادس: معايير وأطر الأمن السيبراني المطبقة في القطاع الحكومي

- المعايير الدولية: مثل ISO/IEC 27001 (نظام إدارة أمن المعلومات)، NIST Cybersecurity Framework.
- المعايير المحلية: أي أطر أو أدلة إرشادية خاصة بالأمن السيبراني صادرة عن الهيئة الوطنية للأمن السيبراني أو جهات حكومية أخرى في المملكة العربية السعودية.
- فوائد تطبيق هذه المعايير: تحسين مستوى الأمان، الامتثال، تعزيز الثقة.

## المحور السابع: تحديات الأمن السيبراني في سياق المشاريع التقنية الحكومية

- نقص الكفاءات: التحدي المتمثل في توفر الكفاءات المتخصصة في الأمن السيبراني.
- الميزانية والموارد: قيود الميزانية المخصصة للأمن السيبراني في المشاريع.
- تطور التهديدات: سرعة تطور التهديدات السيبرانية وصعوبة مواكبتها.
- الوعي وثقافة الأمن: تحديات نشر الوعي وبناء ثقافة أمنية قوية داخل فرق العمل.
- البيروقراطية والإجراءات: تأثير الإجراءات الإدارية على سرعة تطبيق تدابير الأمن السيبراني.

## المحور الثامن: دور العنصر البشري في الأمن السيبراني للمشاريع

- الوعي الأمني: أهمية رفع وعي مديري المشاريع وفرق العمل بالمخاطر الأمنية.
- التدريب والتطوير: ضرورة توفير برامج تدريب مستمرة في مجال الأمن السيبراني.
- المسؤوليات والصلاحيات: تحديد واضح لأدوار ومسؤوليات كل فرد في المشروع تجاه الأمن السيبراني.
- ثقافة الإبلاغ عن الحوادث: تشجيع الإبلاغ الفوري عن أي شبهات أو حوادث أمنية.

المحور التاسع: أفضل الممارسات لتعزيز الأمن السيبراني في إدارة المشاريع

- منهجية DevSecOps: دمج الأمن في كل مرحلة من مراحل التطوير والعمليات.
- إدارة المخاطر السيبرانية المنهجية: تحديد المخاطر، تقييمها، التخفيف منها، ومراقبتها.
- الاختبارات الأمنية الدورية: اختبار الاختراق، فحص الثغرات، ومراجعة الشفرة.
- التعاون والشراكات: أهمية التعاون بين الجهات الحكومية والخاصة وتبادل المعلومات حول التهديدات.

المحور العاشر: الخاتمة

## المحور الأول: مفهوم وأهمية إدارة المشاريع التقنية

### مفهوم إدارة المشاريع

إدارة المشاريع هي تطبيق المعرفة والمهارات والأدوات والتقنيات على أنشطة المشروع لتلبية متطلبات المشروع. الهدف الأساسي هو تحقيق أهداف محددة ضمن قيود معينة مثل الوقت، التكلفة، والنطاق.

### مراحل دورة حياة المشروع:

- البدء (Initiation): هي المرحلة الأولى التي يتم فيها تحديد فكرة المشروع وأهدافه العامة، وتحديد الجدوى الأولية للمشروع. يتم خلالها تحديد أصحاب المصلحة الرئيسيين وتعيين مدير للمشروع.
- التخطيط (Planning): في هذه المرحلة، يتم وضع خطة مفصلة للمشروع تشمل تحديد النطاق، الجداول الزمنية، الميزانية، الموارد المطلوبة، وتحليل المخاطر. الهدف هو تحديد كيفية تحقيق أهداف المشروع.
- التنفيذ (Execution): هي المرحلة التي يتم فيها تنفيذ الأنشطة المخطط لها. يشمل ذلك إدارة الموارد، توجيه فرق العمل، وتنسيق الجهود لتحقيق مخرجات المشروع.
- المراقبة والتحكم (Controlling & Monitoring): هذه المرحلة تتم بالتوازي مع مرحلة التنفيذ، وتهدف إلى تتبع تقدم المشروع ومقارنته بالخطة الموضوعية. يتم

خلالها تحديد الانحرافات واتخاذ الإجراءات التصحيحية لضمان بقاء المشروع على المسار الصحيح.

- الإغلاق (Closing): هي المرحلة النهائية التي يتم فيها إنهاء جميع أنشطة المشروع رسميًا، وتسليم المخرجات النهائية، وإغلاق العقود، وتحرير الموارد، وتوثيق الدروس المستفادة للمشاريع المستقبلية.

### المشاريع التقنية

المشاريع التقنية هي تلك المشاريع التي تركز على تطوير أو تطبيق أو تحسين أنظمة وتطبيقات البنية التحتية التكنولوجية. تشمل هذه المشاريع تطوير البرمجيات، نشر الأنظمة الجديدة، ترقية الشبكات، أو تنفيذ حلول الذكاء الاصطناعي، وغيرها.

خصائص المشاريع التقنية:

- التغير السريع: تتطور التقنيات بوتيرة عالية، مما يتطلب مرونة في التخطيط والتنفيذ.
- التعقيد: غالبًا ما تكون المشاريع التقنية معقدة بسبب تداخل الأنظمة والمكونات المختلفة.
- المخاطر العالية: يمكن أن تواجه تحديات غير متوقعة مثل مشكلات التوافقية أو الثغرات الأمنية.
- الحاجة إلى التخصص: تتطلب فرق عمل ذات مهارات تقنية عالية ومتخصصة.

## تحدياتها:

- إدارة التغيير: صعوبة التكيف مع التغيرات التقنية ومتطلبات العملاء.
  - نقص الموارد: صعوبة العثور على المواهب المتخصصة أو توفر الميزانيات الكافية.
  - المخاطر الأمنية: تزايد التهديدات السيبرانية التي قد تؤثر على سرية وسلامة وتوافر الأنظمة.
  - تجاوز النطاق: ميل بعض المشاريع التقنية للتوسع خارج نطاقها الأصلي.
- أهميتها في تحقيق أهداف المؤسسات:
- تعد المشاريع التقنية حجر الزاوية لتحقيق الأهداف الاستراتيجية للمؤسسات في العصر الرقمي، فهي تمكنها من:
- تحسين الكفاءة التشغيلية.
  - ابتكار منتجات وخدمات جديدة.
  - تعزيز القدرة التنافسية.
  - تحقيق ميزة تنافسية مستدامة.
- فعالية إدارة المشاريع
- تُقاس فعالية إدارة المشاريع بعدة معايير لضمان تحقيق الأهداف المرجوة:

معايير قياس فعالية المشروع:

- الالتزام بالوقت (On-Time Delivery): هل تم تسليم المشروع في الموعد المحدد أو قبله؟
- الميزانية (Within Budget): هل تم إنجاز المشروع ضمن الميزانية المخصصة أو أقل منها؟
- الجودة (Quality): هل تلبى المخرجات المواصفات والمعايير المطلوبة وتوقعات أصحاب المصلحة؟
- رضا أصحاب المصلحة (Stakeholder Satisfaction): هل يشعر أصحاب المصلحة الرئيسيون (العملاء، المستخدمون، الإدارة) بالرضا عن نتائج المشروع؟
- تحقيق أهداف الأعمال (Business Objectives Achievement): هل ساهم المشروع في تحقيق الأهداف الاستراتيجية والتجارية للمؤسسة؟

المحور الثاني: الأمن السيبراني: المفاهيم الأساسية والتهديدات

تعريف الأمن السيبراني

الأمن السيبراني هو مجموعة من التقنيات والعمليات والممارسات المصممة لحماية الأنظمة والشبكات والبرامج والبيانات من الهجمات الرقمية، التلف أو الوصول غير المصرح به.

## المبادئ الأساسية (CIA Triad):

- السرية (Confidentiality): ضمان أن المعلومات لا يمكن الوصول إليها إلا من

قبل الأشخاص المصرح لهم.

- السلامة (Integrity): ضمان أن المعلومات دقيقة وكاملة ولم يتم تعديلها أو

تدميرها بشكل غير مصرح به.

- التوافر (Availability): ضمان أن الأنظمة والمعلومات يمكن الوصول إليها

واستخدامها من قبل الأشخاص المصرح لهم عند الحاجة.

الفرق بين أمن المعلومات والأمن السيبراني:

- أمن المعلومات (Information Security): هو مفهوم أوسع يشمل حماية جميع

أنواع المعلومات (سواء كانت رقمية أو مادية) من الوصول غير المصرح به،

التلف، أو الكشف.

- الأمن السيبراني (Cybersecurity): هو جزء من أمن المعلومات ويركز بشكل

خاص على حماية المعلومات والأنظمة في الفضاء السيبراني (الرقمي).

أهمية الأمن السيبراني

في البيئة الرقمية الحديثة، أصبح الأمن السيبراني ذا أهمية قصوى لعدة أسباب:

- حماية البيانات الحساسة: حماية بيانات العملاء والموظفين والمعلومات التجارية

السرية.

- الأثر على الثقة: فقدان الثقة لدى العملاء والشركاء نتيجة اختراق البيانات.
  - سمعة المؤسسات: تضرر سمعة المؤسسة بشكل كبير بعد حادث أمني.
  - استمرارية الأعمال: ضمان استمرارية العمليات التجارية وتجنب التوقفات المكلفة بسبب الهجمات.
  - الامتثال التنظيمي: الالتزام باللوائح والقوانين المتعلقة بحماية البيانات والخصوصية.
- أنواع التهديدات السيبرانية
- البرمجيات الخبيثة (Malware):
    - الفدية (Ransomware): برنامج يمنع المستخدمين من الوصول إلى أنظمتهم أو بياناتهم حتى يتم دفع فدية.
    - الفيروسات (Viruses): برامج تضر بالملفات أو الأنظمة وتنتشر ذاتيًا.
    - أحصنة طروادة (Trojans): برامج تتنكر كبرامج مشروعة لسرقة البيانات أو السيطرة على النظام.
  - التصيد الاحتيالي (Phishing): محاولات لخداع الأفراد لتقديم معلومات حساسة (مثل أسماء المستخدمين وكلمات المرور) غالبًا عبر رسائل بريد إلكتروني أو رسائل نصية مزيفة.

- هجمات حجب الخدمة الموزعة (DDoS – Distributed Denial of Service): إغراق خادم أو شبكة بكمية هائلة من حركة المرور المزيفة لمنع المستخدمين الشرعيين من الوصول إليها.
- اختراقات البيانات (Data Breaches): الوصول غير المصرح به إلى البيانات الحساسة أو سرقتها من نظام أو شبكة.
- التجسس السيبراني (Cyber Espionage): سرقة معلومات سرية أو حساسة من قبل دول أو جهات حكومية لأغراض سياسية أو اقتصادية.
- الهجمات المتقدمة المستمرة (APT – Advanced Persistent Threats): هجمات معقدة وطويلة الأمد تنفذها مجموعات ذات موارد عالية (غالبًا مدعومة من دول) بهدف التسلل إلى الشبكات والبقاء فيها دون اكتشاف لفتترات طويلة لسرقة البيانات.
- أثر التهديدات على المشاريع التقنية
- المخاطر المباشرة:
  - توقف العمل: تعطل الأنظمة والخدمات، مما يؤدي إلى تأخير المشروع.
  - فقدان البيانات: تدمير أو سرقة بيانات المشروع الهامة.
  - التكاليف الإضافية: تكاليف الاستجابة للحوادث، التعافي، والتحقيقات الجنائية الرقمية.

• المخاطر غير المباشرة:

- فقدان الثقة: تراجع ثقة أصحاب المصلحة في قدرة الفريق على إدارة المشروع بأمان.
- تأثير على السمعة: تضرر سمعة المؤسسة أو فريق المشروع.
- مشكلات قانونية: غرامات وعقوبات نتيجة عدم الامتثال للوائح حماية البيانات.
- إعادة العمل: الحاجة إلى إعادة تصميم أو تطوير مكونات المشروع لتصحيح الثغرات الأمنية.

المحور الثالث: العلاقة بين الأمن السيبراني وإدارة المشاريع

الأمن السيبراني كجزء لا يتجزأ من إدارة المشاريع

في السابق، كان الأمن السيبراني يُنظر إليه غالبًا على أنه "إضافة" أو مرحلة لاحقة في دورة حياة المشروع. ومع تزايد التهديدات وتعقيد الأنظمة، أصبح عنصرًا أساسيًا يجب دمجه في كل مرحلة من مراحل المشروع. هذا التحول يعني أن الأمن لم يعد مسؤولية فريق الأمن فقط، بل هو مسؤولية مشتركة لجميع أفراد فريق المشروع. دمج الأمن منذ البداية يقلل من التكاليف ويحسن من جودة المشروع ومرونته.

تأثير مخاطر الأمن السيبراني على خطط المشروع

مخاطر الأمن السيبراني يمكن أن تؤثر بشكل كبير على جوانب مختلفة من خطة

المشروع:

• الجدولة (Scheduling): قد تؤدي الثغرات الأمنية المكتشفة متأخرًا إلى تأخيرات

كبيرة في الجدولة، حيث يتطلب الأمر وقتًا لتصحيحها وإعادة الاختبار.

• الميزانية (Budget): تتضمن تكاليف الاستجابة للحوادث الأمنية، إعادة التطوير،

التدريب الأمني، وشراء أدوات أمنية إضافية زيادة في الميزانية المخصصة

للمشروع.

• نطاق العمل (Scope): قد تتطلب المتطلبات الأمنية الإضافية أو التهديدات

الجديدة توسيع نطاق العمل ليشمل أنشطة أمنية لم تكن مخططة في البداية.

• إدارة المخاطر (Risk Management): يجب أن تتضمن خطة إدارة المخاطر

تحليلًا مفصلاً لمخاطر الأمن السيبراني، خطط الاستجابة، وتدابير التخفيف.

• إدارة الجودة (Quality Management): الجودة الأمنية هي جزء لا يتجزأ من

الجودة الكلية للمشروع. أي نقص في الأمن يمكن أن يؤثر سلبًا على جودة

المخرجات النهائية.

## الأمن السيبراني كعامل تمكين

بعيداً عن كونه مجرد عبء، يمكن للأمن السيبراني القوي أن يكون عامل تمكين رئيسي

لنجاح المشاريع التقنية:

- بناء الثقة: يعزز الثقة لدى العملاء وأصحاب المصلحة بأن بياناتهم آمنة وأن

المشروع محصن ضد الهجمات.

- الامتثال التنظيمي: يساعد على الامتثال للوائح والمعايير الأمنية، مما يجنب

المؤسسة الغرامات والمشكلات القانونية.

- تقليل المخاطر: يقلل من احتمالية وقوع حوادث أمنية مكلفة ومؤثرة على سير

العمل.

- تعزيز سمعة المؤسسة: يعكس التزام المؤسسة بالمسؤولية والأمان، مما يعزز

سمعتها في السوق.

- الابتكار الآمن: يتيح للمؤسسات الابتكار وتطوير حلول جديدة بثقة، مع ضمان

بناء الأمن في صميم هذه الحلول.

المحور الرابع: الإطار التنظيمي والتشريعي للأمن السيبراني في المملكة العربية السعودية

تولي المملكة العربية السعودية اهتماماً كبيراً للأمن السيبراني كركيزة أساسية لتحقيق

التحول الرقمي ضمن رؤية 2030.

## الهيئة الوطنية للأمن السيبراني (NCA)

- دورها: هي الجهة المختصة في المملكة بالأمن السيبراني، وتتولى مسؤولية تعزيزه وحمايته على المستوى الوطني. تأسست عام 2017 وترتبط مباشرة بالملك.
- استراتيجيتها: تهدف إلى بناء فضاء سيبراني سعودي آمن وموثوق يمكن النمو والازدهار. تركز على تطوير الأطر التنظيمية، بناء القدرات الوطنية، وتعزيز التعاون الدولي.

### • أهدافها:

- وضع السياسات والاستراتيجيات الوطنية للأمن السيبراني.
- بناء وتطوير القدرات الوطنية في مجال الأمن السيبراني.
- حماية الفضاء السيبراني للمملكة والبنى التحتية الحيوية.
- تعزيز الوعي بالأمن السيبراني.
- تشجيع البحث والتطوير والابتكار في المجال.

### اللوائح والسياسات الوطنية

أصدرت الهيئة الوطنية للأمن السيبراني وبعض الجهات الأخرى ذات الصلة (مثل البنك المركزي السعودي - ساما) العديد من اللوائح والإرشادات لتعزيز الأمن السيبراني:

- الضوابط الأساسية للأمن السيبراني ( ECC – Essential Cybersecurity Controls): هي مجموعة من الضوابط الإلزامية التي يجب على الجهات الوطنية الالتزام بها لحماية أصولها السيبرانية. تشمل هذه الضوابط مجالات مثل إدارة المخاطر، إدارة الهوية والوصول، الأمن المادي، وأمن الشبكات.
- المنهجية الوطنية لإدارة المخاطر السيبرانية ( NCERM – National Cybersecurity Risk Management Methodology): توفر إطارًا موحدًا لتقييم وإدارة المخاطر السيبرانية في الجهات الوطنية.
- إطار الحوكمة الوطنية للأمن السيبراني ( NCGF – National Cybersecurity Governance Framework): يحدد مسؤوليات ومستويات الحوكمة اللازمة لتحقيق الأمن السيبراني الفعال.
- معايير الأمن السيبراني للقطاع المالي ( SAMA Cybersecurity Framework): معايير إلزامية للقطاع المالي لضمان حماية البيانات والمعاملات المالية.

## رؤية 2030 والأمن السيبراني

تدعم رؤية المملكة 2030 بناء قطاع رقمي آمن ومرن بشكل مباشر، وذلك من خلال:

- التحول الرقمي الشامل: تعتمد الرؤية بشكل كبير على التحول الرقمي في جميع القطاعات، وهذا يتطلب بيئة سيبرانية آمنة وموثوقة.

- تطوير الاقتصاد الرقمي: تهدف الرؤية إلى تنويع مصادر الدخل وتعزيز الاقتصاد الرقمي، والأمن السيبراني ضروري لجذب الاستثمارات وحماية الابتكارات.
- بناء القدرات الوطنية: تركز الرؤية على تنمية رأس المال البشري وتوطين التقنيات، بما في ذلك بناء الكفاءات في مجال الأمن السيبراني.
- حماية البنى التحتية الحيوية: الأمن السيبراني محوري لحماية البنى التحتية الوطنية الحيوية مثل الطاقة، المياه، والنقل، والتي تعد أساسًا لتحقيق أهداف الرؤية.
- تعزيز الثقة الرقمية: تسعى الرؤية إلى بناء مجتمع رقمي واثق، وهذا يتطلب بيئة رقمية آمنة يمكن للمواطنين والمقيمين والشركات الوثوق بها.

المحور الخامس: تكامل الأمن السيبراني في مراحل دورة حياة المشروع

لضمان نجاح المشاريع التقنية ومرونتها، يجب دمج اعتبارات الأمن السيبراني في كل مرحلة من مراحل دورة حياة المشروع.

الأمن في مرحلة البدء والتخطيط

هذه المراحل حاسمة لوضع أسس الأمن السيبراني للمشروع:

- تحديد المتطلبات الأمنية:

◦ في مرحلة البدء: تحديد المتطلبات الأمنية الأولية بناءً على طبيعة المشروع

والبيانات التي سيتعامل معها (مثل متطلبات السرية، السلامة، التوافر).

◦ في مرحلة التخطيط: يتم تحديد المتطلبات الأمنية بشكل أكثر تفصيلاً،

بالتشاور مع خبراء الأمن وأصحاب المصلحة، مع الأخذ في الاعتبار

اللوائح والمعايير ذات الصلة (مثل ضوابط NCA).

• تحليل المخاطر الأولية:

◦ تحديد التهديدات ونقاط الضعف المحتملة التي قد تواجه المشروع.

◦ تقييم احتمالية حدوث المخاطر وتأثيرها المحتمل.

◦ وضع استراتيجيات مبدئية للتخفيف من هذه المخاطر أو التعامل معها.

• الموازنة بين الأهداف الأمنية وأهداف المشروع:

◦ من المهم تحقيق توازن بين المتطلبات الأمنية وأهداف المشروع الأخرى

(الوقت، التكلفة، النطاق). قد تتطلب الإجراءات الأمنية موارد إضافية،

ويجب تخصيص هذه الموارد في خطة المشروع.

◦ يتم دمج خطة الأمن السيراني كجزء من خطة المشروع الرئيسية.

الأمن في مرحلة التنفيذ

في هذه المرحلة، يتم تحويل المتطلبات الأمنية إلى واقع عملي:

• التطوير الآمن (Secure Development Life Cycle – SDLC):

- دمج الممارسات الأمنية في كل خطوة من خطوات دورة حياة تطوير البرمجيات، بدءًا من التصميم وحتى الاختبار.
- تضمين تحليل التهديدات ونقاط الضعف (Threat Modeling) في مرحلة التصميم.
- استخدام مبادئ التصميم الآمن (مثل مبدأ الامتياز الأقل).
- التدريب المستمر للمطورين على ممارسات البرمجة الآمنة.

• الاختبار الأمني:

- إجراء اختبارات اختراق (Penetration Testing) لتحديد الثغرات الأمنية التي يمكن استغلالها من قبل المهاجمين.
- القيام باختبارات الضعف (Vulnerability Scanning) لتحديد نقاط الضعف المعروفة.
- إجراء مراجعة الشفرة المصدرية (Code Review) لاكتشاف الأخطاء الأمنية في الكود.
- الاختبار الوظيفي للأمن للتأكد من أن آليات التحكم الأمني تعمل كما هو متوقع.

- إدارة الثغرات (Vulnerability Management):

- وضع عملية لتحديد الثغرات الأمنية وتصنيفها ومعالجتها بشكل فعال وفي

- الوقت المناسب.

- تطبيق التصحيحات (Patches) والتحديثات الأمنية بانتظام.

- الأمن في مرحلة المراقبة والإغلاق

- هذه المراحل تضمن استمرارية الأمن وتحسين الممارسات المستقبلية:

- المراقبة الأمنية المستمرة (Continuous Security Monitoring):

- مراقبة الأنظمة والشبكات للكشف عن أي نشاط مشبوه أو هجمات سيبرانية

- في الوقت الفعلي.

- استخدام أنظمة إدارة المعلومات الأمنية والأحداث (SIEM) لتجميع وتحليل

- سجلات الأمن.

- الاستعداد للاستجابة السريعة لأي حادث أمني.

- إدارة الحوادث (Incident Management):

- وضع خطة واضحة للاستجابة للحوادث الأمنية، تتضمن خطوات الكشف،

- الاحتواء، الاستئصال، التعافي، والدروس المستفادة.

◦ إجراء تمارين محاكاة للحوادث (Incident Response Drills) لتدريب

الفرق على الاستجابة الفعالة.

• التوثيق (Documentation):

◦ توثيق جميع الإجراءات والقرارات الأمنية المتخذة خلال دورة حياة المشروع.

◦ توثيق الثغرات المكتشفة وكيفية معالجتها.

◦ توثيق خطط الاستجابة للحوادث والسياسات الأمنية.

• الدروس المستفادة (Lessons Learned):

◦ في مرحلة الإغلاق، يتم مراجعة الأداء الأمني للمشروع وتحديد ما تم عمله

بشكل جيد وما يحتاج إلى تحسين.

◦ توثيق هذه الدروس المستفادة لتطبيقها في المشاريع المستقبلية وتحسين

ممارسات الأمن السيبراني المؤسسية.

المحور السادس: معايير وأطر الأمن السيبراني المطبقة في القطاع الحكومي

لضمان بيئة رقمية آمنة وموثوقة، تعتمد الجهات الحكومية على مجموعة من المعايير والأطر التي توجه ممارسات الأمن السيبراني.

#### المعايير الدولية

• ISO/IEC 27001 (نظام إدارة أمن المعلومات - ISMS):

- هو معيار دولي يحدد المتطلبات اللازمة لإنشاء وتنفيذ وصيانة وتحسين مستمر لنظام إدارة أمن المعلومات في المؤسسة.
- لا يحدد هذا المعيار ضوابط أمنية محددة، ولكنه يوفر إطارًا لتحديد وإدارة المخاطر الأمنية بشكل منهجي.
- يساعد المؤسسات على حماية معلوماتها الحساسة من خلال نهج قائم على المخاطر. الحصول على شهادة ISO 27001 يظهر التزام المؤسسة بأفضل ممارسات أمن المعلومات.

• NIST Cybersecurity Framework (إطار عمل NIST للأمن السيبراني):

- هو إطار عمل طوعي قائم على المعايير والإرشادات والممارسات الموجودة لمساعدة المؤسسات على إدارة وتقليل مخاطر الأمن السيبراني.

○ يتكون الإطار من خمس وظائف أساسية: تحديد (Identify)، حماية

(Protect)، كشف (Detect)، استجابة (Respond)، تعافي

(Recover).

○ يستخدم هذا الإطار على نطاق واسع في القطاعين العام والخاص في

جميع أنحاء العالم لتقييم وتحسين برامج الأمن السيبراني.

#### المعايير المحلية

في المملكة العربية السعودية، تلعب الهيئة الوطنية للأمن السيبراني (NCA) دورًا محوريًا

في وضع الأطر واللوائح المحلية:

• الضوابط الأساسية للأمن السيبراني (ECC – Essential Cybersecurity

Controls):

○ هي مجموعة إلزامية من الضوابط والمعايير التي يجب على الجهات

الوطنية في المملكة الالتزام بها لحماية أنظمتها وبياناتها.

○ تغطي هذه الضوابط مجالات مثل حوكمة الأمن السيبراني، إدارة المخاطر،

إدارة أمن الأصول، أمن الموارد البشرية، أمن العمليات، أمن الشبكات

والأنظمة، وأمن المعلومات والبيانات.

○ تهدف إلى رفع مستوى الأمن السيبراني على المستوى الوطني وتوفير حد

أدنى من الحماية لجميع الجهات.

• المنهجية الوطنية لإدارة المخاطر السيبرانية ( NCERM – National )

:(Cybersecurity Risk Management Methodology

◦ إطار عمل موحد لتحديد وتقييم وإدارة المخاطر السيبرانية على مستوى الجهات الوطنية.

◦ تساعد الجهات على فهم المخاطر التي تواجهها وتطوير استراتيجيات فعالة للتخفيف منها.

• إطار الحوكمة الوطنية للأمن السيبراني ( NCGF – National )

:(Cybersecurity Governance Framework

◦ يحدد هذا الإطار الهيكل التنظيمي والمسؤوليات والصلاحيات اللازمة لضمان حوكمة فعالة للأمن السيبراني داخل الجهات الوطنية.

◦ يضمن وجود قيادة واضحة ومسائلة في مجال الأمن السيبراني.

فوائد تطبيق هذه المعايير

• تحسين مستوى الأمان: تساهم هذه الأطر في بناء دفاعات قوية ضد التهديدات

السيبرانية، مما يقلل من احتمالية وقوع الحوادث الأمنية ويحسن قدرة المؤسسات

على التعافي منها.

- الامتثال (Compliance): يساعد تطبيق هذه المعايير على ضمان امتثال الجهات للوائح والقوانين المحلية والدولية المتعلقة بحماية البيانات والأمن السيبراني، مما يجنبها الغرامات والعقوبات القانونية.
- تعزيز الثقة: يعزز تطبيق المعايير الثقة لدى المواطنين، الشركاء، والمستثمرين في قدرة الجهات الحكومية على حماية بياناتهم وأنظمتهم، مما يدعم مسيرة التحول الرقمي والتنمية الاقتصادية.
- إدارة المخاطر الفعالة: توفر نهجًا منظمًا لتحديد وتقييم ومعالجة المخاطر السيبرانية، مما يمكن الجهات من اتخاذ قرارات مستنيرة بشأن استثماراتها الأمنية.

المحور السابع: تحديات الأمن السيبراني في سياق المشاريع التقنية الحكومية

على الرغم من الأهمية المتزايدة للأمن السيبراني، تواجه المشاريع التقنية الحكومية تحديات متعددة في هذا المجال:

- نقص الكفاءات:
  - التحدي: هناك فجوة عالمية في عدد المتخصصين في الأمن السيبراني المؤهلين، وهذا التحدي يتفاقم في القطاع الحكومي حيث قد تكون الرواتب والمزايا أقل تنافسية مقارنة بالقطاع الخاص.

○ التأثير: يؤدي نقص الكفاءات إلى صعوبة في بناء فرق أمن سيبراني قوية داخل المشاريع، وتأخير في تنفيذ تدابير الأمن، وقد يترك ثغرات أمنية غير مكتشفة.

• الميزانية والموارد:

○ التحدي: غالبًا ما تواجه المشاريع الحكومية قيودًا صارمة على الميزانية، مما قد يؤثر على القدرة على شراء أحدث التقنيات الأمنية، وتوظيف الخبراء، وتوفير التدريب اللازم.

○ التأثير: قد تضطر المشاريع إلى التنازل عن بعض تدابير الأمن أو استخدام حلول أقل فعالية، مما يزيد من تعرضها للمخاطر.

• تطور التهديدات:

○ التحدي: تتطور التهديدات السيبرانية (مثل هجمات الفدية، التصيد الاحتيالي، الهجمات المتقدمة المستمرة) بوتيرة سريعة جدًا، مما يجعل من الصعب على الجهات الحكومية مواكبة هذه التهديدات وتطوير دفاعات فعالة في الوقت المناسب.

○ التأثير: قد تصبح الأنظمة والمشاريع القديمة أو التي لا يتم تحديثها بانتظام عرضة لهجمات جديدة.

• الوعي وثقافة الأمن:

- التحدي: على الرغم من الجهود المبذولة، لا يزال هناك نقص في الوعي الأمني بين بعض الموظفين، وهذا يشمل مديري المشاريع وفرق العمل التقنية. قد لا يدركون أهمية دورهم في الحفاظ على الأمن.
- التأثير: يمكن أن يكون العنصر البشري أضعف حلقة في سلسلة الأمن، حيث يمكن أن تؤدي الأخطاء البشرية (مثل النقر على روابط التصيد) إلى اختراقات أمنية خطيرة.

• البيروقراطية والإجراءات:

- التحدي: في بعض الأحيان، يمكن أن تؤدي الإجراءات الإدارية المعقدة والبطيئة في القطاع الحكومي إلى تأخير في الموافقة على الميزانيات الأمنية، شراء الحلول، أو تنفيذ التغييرات اللازمة لتعزيز الأمن.
- التأثير: هذه التأخيرات يمكن أن تجعل المشاريع عرضة للتهديدات لفترات أطول، أو تمنع تطبيق أفضل الممارسات الأمنية في الوقت المناسب.

المحور الثامن: دور العنصر البشري في الأمن السيبراني للمشاريع

يُعد العنصر البشري حجر الزاوية في أي استراتيجية أمن سيبراني ناجحة. فمهما كانت التقنيات المطبقة متطورة، يظل السلوك البشري عاملاً حاسماً في تحديد مدى فعالية الأمن.

• الوعي الأمني (Security Awareness):

- الأهمية: يجب رفع مستوى الوعي الأمني لجميع أفراد فريق المشروع، من مدير المشروع إلى المطورين والمستخدمين. يجب أن يفهم الجميع المخاطر المحتملة، وكيف يمكن أن تؤثر الهجمات السيبرانية على المشروع، وما هو دورهم في الحماية.

- التطبيق: يمكن تحقيق ذلك من خلال حملات توعية منتظمة، ورسائل بريد إلكتروني، وملصقات، ومحاضرات قصيرة. يجب أن يركز الوعي على المخاطر الشائعة مثل التصيد الاحتيالي، الهندسة الاجتماعية، أهمية كلمات المرور القوية، والتعامل الآمن مع البيانات الحساسة.

• التدريب والتطوير (Training and Development):

- الضرورة: الوعي وحده لا يكفي. يجب توفير برامج تدريب متخصصة ومستمرة تتناسب مع أدوار الأفراد.
- أمثلة:

- لمديري المشاريع: تدريب على إدارة مخاطر الأمن السيبراني، دمج الأمن في خطط المشروع، وتحديد المتطلبات الأمنية.

- للمطورين: تدريب على ممارسات البرمجة الآمنة ( Secure Coding Practices)، اكتشاف الثغرات الشائعة (مثل OWASP Top 10)، وأدوات تحليل الكود.
- لمتخصصي الشبكات والأنظمة: تدريب على تأمين البنية التحتية، إدارة التهديدات، والاستجابة للحوادث.
- المسؤوليات والصلاحيات (Roles and Responsibilities):
  - التحديد الواضح: يجب تحديد أدوار ومسؤوليات كل فرد في المشروع تجاه الأمن السيبراني بوضوح. من المسؤول عن أمن البيانات؟ من يقوم بمراجعة الكود الأمني؟ من يراقب السجلات الأمنية؟
  - التطبيق: هذا يضمن عدم وجود ثغرات في المسؤولية ويقلل من الارتباك، مما يعزز المساءلة ويضمن تنفيذ تدابير الأمن بفعالية.
- ثقافة الإبلاغ عن الحوادث (Incident Reporting Culture):
  - التشجيع: يجب تشجيع الموظفين على الإبلاغ الفوري عن أي شبهات أو حوادث أمنية، مهما بدت صغيرة. الخوف من العقاب أو عدم اليقين قد يؤدي إلى إخفاء الحوادث، مما يزيد من الأضرار.

○ التطبيق: إنشاء قنوات واضحة وموثوقة للإبلاغ، وتأكيد أن الإبلاغ يتم دون

لوم (No-Blame Culture) مع التركيز على التعلم والتحسين. هذا

يساعد على الكشف المبكر عن التهديدات والاستجابة السريعة لها.

المحور التاسع: أفضل الممارسات لتعزيز الأمن السيبراني في إدارة المشاريع

لتحقيق أقصى قدر من الأمن في المشاريع التقنية، يجب تبني أفضل الممارسات التي

تدمج الأمن كجزء أساسي من العملية:

• منهجية (DevSecOps (Development, Security, and Operations):

○ المفهوم: هي امتداد لمفهوم DevOps، حيث يتم دمج الأمن في كل مرحلة

من مراحل دورة حياة التطوير والعمليات، وليس كمرحلة لاحقة. "الأمن يبدأ

من التصميم" (Security by Design).

○ التطبيق:

▪ في التصميم: دمج تحليل التهديدات ونماذج الأمان.

▪ في التطوير: استخدام أدوات تحليل الكود الثابت (SAST)

والديناميكي (DAST)، وتدريب المطورين على البرمجة الآمنة.

▪ في الاختبار: إجراء اختبارات اختراق منتظمة وفحص الثغرات.

- في النشر والعمليات: أتمتة عمليات نشر التحديثات الأمنية، والمراقبة المستمرة، وإدارة الثغرات.
- الفوائد: الكشف عن الثغرات مبكرًا (مما يقلل التكلفة)، تسريع دورة التسليم، وتعزيز جودة وأمان المنتج النهائي.
- إدارة المخاطر السيبرانية المنهجية:
  - المفهوم: اعتماد نهج منظم ومستمر لتحديد، تقييم، التخفيف، ومراقبة المخاطر السيبرانية على مدار دورة حياة المشروع بأكملها.
  - التطبيق:
  - التحديد: تحديد الأصول الحساسة والتهديدات المحتملة ونقاط الضعف.
  - التقييم: تقييم احتمالية حدوث المخاطر وتأثيرها على المشروع.
  - التخفيف: تطوير وتنفيذ استراتيجيات للتخفيف من المخاطر (مثل تطبيق ضوابط أمنية، تحديث الأنظمة).
  - المراقبة: مراقبة المخاطر باستمرار وتقييم فعالية تدابير التخفيف، وتحديث سجل المخاطر.
  - الفوائد: اتخاذ قرارات مستنيرة بشأن الأمن، تخصيص الموارد بكفاءة، وتقليل التعرض للخسائر المحتملة.

- الاختبارات الأمنية الدورية:

- الضرورة: يجب أن تكون الاختبارات الأمنية جزءًا لا يتجزأ من جدول

المشروع، لا مجرد خطوة تتم لمرة واحدة.

- أنواع الاختبارات:

- اختبار الاختراق (Penetration Testing): محاكاة هجمات

حقيقية لتحديد الثغرات الأمنية القابلة للاستغلال.

- فحص الثغرات (Vulnerability Scanning): استخدام أدوات آلية

لتحديد نقاط الضعف المعروفة في الأنظمة والشبكات.

- مراجعة الشفرة (Code Review): فحص الشفرة المصدرية يدويًا

أو باستخدام أدوات آلية لاكتشاف الثغرات الأمنية في التصميم

والتنفيذ.

- الفوائد: تحديد الثغرات قبل أن يستغلها المهاجمون، وتحسين جودة وأمان

المنتج النهائي.

- التعاون والشراكات:

- الأهمية: في بيئة التهديدات المتغيرة باستمرار، يعد التعاون وتبادل

المعلومات أمرًا حيويًا.

- التطبيق:

- بين الجهات الحكومية: تبادل المعلومات حول التهديدات، أفضل الممارسات، والدروس المستفادة من الحوادث الأمنية.
- مع القطاع الخاص: الاستفادة من خبرات الشركات المتخصصة في الأمن السيبراني، والحصول على أحدث الحلول والتقنيات.
- مع المراكز الوطنية للأمن السيبراني: مثل الهيئة الوطنية للأمن السيبراني لتلقي التوجيهات والتنبيهات الأمنية.
- الفوائد: تعزيز الوعي المشترك بالمخاطر، الاستفادة من الخبرات المتبادلة، وتحسين القدرة الجماعية على الاستجابة للتهديدات.

#### المحور العاشر: الخاتمة

لقد أصبح الأمن السيبراني ليس مجرد "إضافة" تقنية، بل عنصرًا حيويًا وأساسيًا في صميم نجاح أي مشروع تقني، خاصة في القطاع الحكومي. لقد استعرضنا في هذا الشرح المفصل مفهوم إدارة المشاريع التقنية وأهميتها، وتعمقنا في أساسيات الأمن السيبراني وأنواع تهديداته.

كما سلطنا الضوء على العلاقة المتداخلة والضرورية بين الأمن السيبراني وإدارة المشاريع، وكيف يمكن لمخاطر الأمن السيبراني أن تؤثر على جميع جوانب المشروع، وكيف يمكن للأمن القوي أن يكون عامل تمكين للنجاح. استعرضنا أيضًا الإطار التنظيمي والتشريعي

القوي الذي وضعته المملكة العربية السعودية، ممثلة بالهيئة الوطنية للأمن السيبراني، لتعزيز الأمن السيبراني كجزء لا يتجزأ من رؤية 2030 الطموحة.

أخيراً، ناقشنا أهمية دمج الأمن السيبراني في كل مرحلة من مراحل دورة حياة المشروع، من البدء والتخطيط إلى التنفيذ والمراقبة والإغلاق، مع التركيز على دور العنصر البشري كخط دفاع أول وأخير، وأفضل الممارسات التي تضمن بناء مشاريع قوية ومحصنة.

إن دمج الأمن السيبراني بشكل استباقي ومنهجي في إدارة المشاريع التقنية الحكومية ليس خياراً، بل ضرورة استراتيجية لضمان حماية الأصول الوطنية، تعزيز الثقة الرقمية، وتحقيق أهداف التحول الرقمي والتنمية المستدامة للمملكة.

## الفصل الرابع

## منهجية الدراسة وطرق البحث

تعتمد هذه الدراسة على المنهج الوصفي التحليلي ( Descriptive Analytical Approach)، الذي يهدف إلى وصف وتحليل أثر الأمن السيبراني على فعالية إدارة المشاريع التقنية في القطاع الحكومي بالمملكة العربية السعودية. سيتم استخدام هذا المنهج لجمع البيانات وتحليلها بشكل منظم وموضوعي للإجابة على تساؤلات الدراسة واختبار فرضياتها.

## مجتمع الدراسة

يتكون مجتمع الدراسة (Study Population) من جميع الأفراد العاملين في إدارة المشاريع التقنية والأمن السيبراني، أو ذوي الصلة المباشرة بهما، في القطاع الحكومي بالمملكة العربية السعودية. يشمل ذلك على سبيل المثال لا الحصر:

- مدراء المشاريع التقنية.
- مهندسي الأمن السيبراني ومتخصصيه.
- أعضاء فرق عمل المشاريع التقنية.
- المسؤولين عن تقنية المعلومات والأمن السيبراني في الهيئات والوزارات الحكومية.

نظراً لحجم مجتمع الدراسة الكبير وتوزعه الجغرافي، سيتم الاعتماد على العينة (Sample) لتمثيل هذا المجتمع. سيتم تحديد حجم العينة وطريقة اختيارها في مرحلة لاحقة لضمان تمثيلها ودلالاتها الإحصائية.

#### أداة الدراسة

ستكون الاستبانة (Questionnaire) هي الأداة الرئيسية لجمع البيانات في هذه الدراسة. سيتم تصميم الاستبانة بعناية لتغطية جميع محاور الدراسة وأهدافها وتساؤلاتها، وستتضمن مجموعة من الأسئلة المغلقة (بأسلوب ليكرت الخماسي) لتقييم آراء وتصورات أفراد عينة الدراسة حول:

- مدى تكامل مبادئ ومعايير الأمن السيبراني في مراحل تخطيط وتنفيذ المشاريع.
- تأثير الالتزام بمعايير الأمن السيبراني على مؤشرات أداء المشاريع (الوقت، التكلفة، الجودة).
- أبرز التحديات الأمنية السيبرانية وتأثيرها على فعالية المشاريع.
- مستوى الوعي والتدريب في مجال الأمن السيبراني.

قبل التطبيق النهائي، سيتم إجراء اختبار مبدئي (Pilot Study) للاستبانة على عينة صغيرة للتأكد من وضوح الأسئلة، سهولة فهمها، ومدى قدرتها على قياس ما وضعت

لقياسه (صدق وثبات الأداة). سيتم تعديل الاستبانة بناءً على نتائج الاختبار المبدئي لضمان فعاليتها.

### جمع البيانات وتحليلها

- جمع البيانات: سيتم توزيع الاستبانة إلكترونياً أو ورقياً على أفراد عينة الدراسة. سيتم الحرص على توفير تعليمات واضحة للمشاركين لضمان دقة الإجابات وسرية المعلومات.
- تحليل البيانات: سيتم استخدام حزم برامج الإحصاء (مثل SPSS) لتحليل البيانات الكمية التي تم جمعها من الاستبانات. ستشمل أساليب التحليل الإحصائي:
  - الإحصاء الوصفي: لحساب التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية لوصف خصائص عينة الدراسة والإجابات على محاور الاستبانة.
  - الإحصاء الاستدلالي: لاختبار فرضيات الدراسة وتحديد العلاقات بين المتغيرات. قد يشمل ذلك تحليل الانحدار المتعدد، اختبار (T-test)، وتحليل التباين (ANOVA) حسب طبيعة البيانات والفرضيات.

تهدف هذه المنهجية إلى توفير إطار عمل شامل وموثوق لإجراء الدراسة وتقديم نتائج دقيقة وموثوقة تسهم في فهم أعمق للعلاقة بين الأمن السيبراني وفعالية إدارة المشاريع التقنية في القطاع الحكومي بالمملكة العربية السعودية.

#### حدود الدراسة

- الحدود الموضوعية: تقتصر الدراسة على تأثير الأمن السيبراني على فعالية إدارة المشاريع التقنية. لن تتناول جوانب أخرى من إدارة المشاريع لا ترتبط بشكل مباشر بالأمن السيبراني، أو قضايا الأمن السيبراني التي لا تؤثر على المشاريع.
- الحدود المكانية: تقتصر الدراسة على القطاع الحكومي في المملكة العربية السعودية. لن يتم تضمين القطاع الخاص أو أي قطاعات حكومية في دول أخرى.
- الحدود الزمانية: ستُجرى الدراسة خلال فترة زمنية ٢٠٢٥

استبيان

الهدف العام للاستبيان:

يهدف هذا الاستبيان إلى جمع البيانات حول مدى تأثير ممارسات وتحديات الأمن السيبراني على فعالية إدارة المشاريع التقنية في الجهات الحكومية بالمملكة العربية السعودية، وذلك لتحديد العلاقة بينهما واقتراح توصيات لتحسين الأداء.

تعليمات:

يرجى قراءة كل عبارة بعناية واختيار الإجابة التي تعبر عن رأيك أو واقع الحال بأكبر دقة، باستخدام المقياس التالي:

(1) غير موافق بشدة (2) غير موافق (3) محايد (4) موافق (5) موافق بشدة

المحور الأول: تكامل الأمن السيبراني في مراحل المشروع

1. يتم دمج متطلبات الأمن السيبراني في مرحلة تخطيط المشاريع التقنية لدينا.

(1) (2) (3) (4) (5)

2. يشارك متخصصو الأمن السيبراني بفعالية في جميع مراحل دورة حياة المشروع التقني.

(1) (2) (3) (4) (5)

3. يتم إجراء تقييمات للمخاطر الأمنية السيبرانية بشكل دوري خلال تنفيذ المشاريع.

(1) (2) (3) (4) (5)

المحور الثاني: الالتزام بمعايير الأمن السيبراني وتأثيره على الأداء

4. تلتزم مشاريعنا التقنية بالمعايير الوطنية والدولية للأمن السيبراني (مثل ISO 27001، CIS Controls).

(1) (2) (3) (4) (5)

5. الالتزام بمعايير الأمن السيبراني يساهم في تسليم المشاريع التقنية في الوقت المحدد.

(1) (2) (3) (4) (5)

6. الالتزام بمعايير الأمن السيبراني يساعد في الالتزام بالميزانية المخصصة للمشاريع التقنية.

(1) (2) (3) (4) (5)

7. الالتزام بمعايير الأمن السيبراني يرفع من جودة مخرجات المشاريع التقنية.

(1) (2) (3) (4) (5)

المحور الثالث: التحديات الأمنية السيبرانية وتأثيرها على الفعالية

8. نواجه تحديات متكررة تتعلق بهجمات التصيد الاحتيالي أو البرمجيات الخبيثة في

مشاريعنا.

(1) (2) (3) (4) (5)

9. تؤدي الاختراقات الأمنية السيبرانية إلى تأخيرات في جداول المشاريع التقنية.

(1) (2) (3) (4) (5)

10. تؤدي الحوادث الأمنية السيبرانية إلى زيادة في تكاليف المشاريع التقنية.

(1) (2) (3) (4) (5)

11. تؤثر التهديدات السيبرانية على جودة أو موثوقية الأنظمة التي يتم تطويرها.

(1) (2) (3) (4) (5)

#### المحور الرابع: الوعي والتدريب في الأمن السيبراني

12. يتلقى فريق عمل المشروع تدريباً كافياً حول أفضل ممارسات الأمن

السيبراني.

(1) (2) (3) (4) (5)

13. يوجد وعي عالٍ بأهمية الأمن السيبراني بين جميع أصحاب المصلحة في

المشاريع التقنية.

(1) (2) (3) (4) (5)

## الفصل الرابع

## التحليل الإحصائي للاستبيان

تم جمع 100 استجابة من المشاركين في القطاع الحكومي بالمملكة العربية السعودية. يهدف هذا التحليل إلى تقديم لمحة سريعة عن التصورات والآراء المتعلقة بتأثير الأمن السيبراني على فعالية إدارة المشاريع التقنية.

المحور الأول: تكامل الأمن السيبراني في مراحل المشروع

يعكس هذا المحور مدى دمج ممارسات الأمن السيبراني في مراحل تخطيط وتنفيذ المشاريع.

| العبارة    | غير موافق بشدة (1) | غير موافق (2) | محايد (3) | موافق (4) | موافق بشدة (5) | المتوسط الحسابي | الانحراف المعياري |
|------------|--------------------|---------------|-----------|-----------|----------------|-----------------|-------------------|
| 1. يتم دمج | 5                  | 10            | 15        | 45        | 25             | 3.85            | 1.12              |

| العبارة                                                        | غير موافق بشدة (1) | غير موافق (2) | محايد (3) | موافق (4) | موافق بشدة (5) | المتوسط الحسابي | الانحراف المعياري |
|----------------------------------------------------------------|--------------------|---------------|-----------|-----------|----------------|-----------------|-------------------|
| متطلبات الأمن السيبراني في مرحلة تخطيط المشاريع التقنية لدينا. |                    |               |           |           |                |                 |                   |
| 2. يشارك متخصص و الأمن                                         | 10                 | 15            | 20        | 35        | 20             | 3.40            | 1.25              |

| الانحراف المعياري | المتوسط الحسابي | موافق بشدة (5) | موافق (4) | محايد (3) | غير موافق (2) | غير موافق بشدة (1) | العبارات                                                                    |
|-------------------|-----------------|----------------|-----------|-----------|---------------|--------------------|-----------------------------------------------------------------------------|
|                   |                 |                |           |           |               |                    | السيبراني<br>بفعالية في<br>جميع<br>مراحل<br>دورة حياة<br>المشروع<br>التقني. |
| 1.19              | 3.64            | 22             | 40        | 18        | 12            | 8                  | 3. يتم<br>إجراء<br>تقييمات<br>للمخاطر                                       |

|            |                    |               |           |           |                |                 |                   |
|------------|--------------------|---------------|-----------|-----------|----------------|-----------------|-------------------|
| العبارة    | غير موافق بشدة (1) | غير موافق (2) | محايد (3) | موافق (4) | موافق بشدة (5) | المتوسط الحسابي | الانحراف المعياري |
| الأمنية    |                    |               |           |           |                |                 |                   |
| السيبرانية |                    |               |           |           |                |                 |                   |
| بشكل       |                    |               |           |           |                |                 |                   |
| دوري       |                    |               |           |           |                |                 |                   |
| خلال       |                    |               |           |           |                |                 |                   |
| تنفيذ      |                    |               |           |           |                |                 |                   |
| المشاريع.  |                    |               |           |           |                |                 |                   |

التحليل الأولي: يظهر متوسط قدره 3.85 للعبارة الأولى أن هناك موافقة عامة على دمج

متطلبات الأمن السيبراني في مرحلة التخطيط. ومع ذلك، ينخفض المتوسط إلى 3.40

للعبارة الثانية، مما يشير إلى أن مشاركة متخصصي الأمن السيبراني قد لا تكون بفعالية

كافية في جميع مراحل المشروع.

المحور الثاني: الالتزام بمعايير الأمن السيبراني وتأثيره على الأداء

يركز هذا المحور على مدى الالتزام بالمعايير الأمنية وتأثير ذلك على مؤشرات أداء

المشروع (الوقت، التكلفة، الجودة).

| العبارة                                                               | غير موافق بشدة (1) | غير موافق (2) | محايد (3) | موافق (4) | موافق بشدة (5) | المتوسط الحسابي | الانحراف المعياري |
|-----------------------------------------------------------------------|--------------------|---------------|-----------|-----------|----------------|-----------------|-------------------|
| 4. تلتزم مشاريعنا التقنية بالمعايير الوطنية والدولية للأمن السيبراني. | 7                  | 13            | 20        | 38        | 22             | 3.55            | 1.20              |

| العبارة                                                                              | غير موافق بشدة (1) | غير موافق (2) | محايد (3) | موافق (4) | موافق بشدة (5) | المتوسط الحسابي | الانحراف المعياري |
|--------------------------------------------------------------------------------------|--------------------|---------------|-----------|-----------|----------------|-----------------|-------------------|
| 5. الالتزام بمعايير الأمن السيبراني يساهم في تسليم المشاريع التقنية في الوقت المحدد. | 10                 | 15            | 25        | 30        | 20             | 3.35            | 1.28              |

| العبارة                                                                                         | غير موافق بشدة (1) | غير موافق (2) | محايد (3) | موافق (4) | موافق بشدة (5) | المتوسط الحسابي | الانحراف المعياري |
|-------------------------------------------------------------------------------------------------|--------------------|---------------|-----------|-----------|----------------|-----------------|-------------------|
| 6. الالتزام بمعايير الأمن السيبراني يساعد في الالتزام بالميزانية المخصصة<br>ة للمشاريع التقنية. | 12                 | 18            | 25        | 28        | 17             | 3.20            | 1.30              |

| العبارة                                                                   | غير موافق بشدة (1) | غير موافق (2) | محايد (3) | موافق (4) | موافق بشدة (5) | المتوسط الحسابي | الانحراف المعياري |
|---------------------------------------------------------------------------|--------------------|---------------|-----------|-----------|----------------|-----------------|-------------------|
| 7. الالتزام بمعايير الأمن السيبراني يرفع من جودة مخرجات المشاريع التقنية. | 6                  | 9             | 15        | 45        | 25             | 3.80            | 1.10              |

التحليل الأولي: يشير متوسط 3.55 للعبارة الرابعة إلى وجود مستوى معقول من الالتزام

بالمعايير. المثير للاهتمام هو أن الالتزام بمعايير الأمن السيبراني يُنظر إليه على أنه

يؤثر بشكل أكبر على الجودة (متوسط 3.80) منه على الالتزام بالوقت (متوسط 3.35)

أو التكلفة (متوسط 3.20)، مما قد يشير إلى تحديات في الموازنة بين المتطلبات الأمنية وجدولة المشاريع وميزانياتها.

المحور الثالث: التحديات الأمنية السيبرانية وتأثيرها على الفعالية

يستكشف هذا المحور التحديات الفعلية التي تواجه المشاريع وكيف تؤثر على فعاليتها.

| العبارة                                    | غير موافق بشدة (1) | غير موافق (2) | محايد (3) | موافق (4) | موافق بشدة (5) | المتوسط الحسابي | الانحراف المعياري |
|--------------------------------------------|--------------------|---------------|-----------|-----------|----------------|-----------------|-------------------|
| 8. نواجه تحديات متكررة تتعلق بهجمات التصيد | 15                 | 20            | 30        | 25        | 10             | 2.95            | 1.25              |

|                   |                 |                |           |           |               |                    |                                             |
|-------------------|-----------------|----------------|-----------|-----------|---------------|--------------------|---------------------------------------------|
| الانحراف المعياري | المتوسط الحسابي | موافق بشدة (5) | موافق (4) | محايد (3) | غير موافق (2) | غير موافق بشدة (1) | العبارة                                     |
|                   |                 |                |           |           |               |                    | الاحتمالي أو البرمجيات الخبيثة في مشاريعنا. |
| 1.20              | 3.62            | 25             | 40        | 15        | 12            | 8                  | 9. تؤدي الاختراقات الأمنية السيبرانية       |

|                   |                 |                |           |           |               |                    |                                                  |
|-------------------|-----------------|----------------|-----------|-----------|---------------|--------------------|--------------------------------------------------|
| الانحراف المعياري | المتوسط الحسابي | موافق بشدة (5) | موافق (4) | محايد (3) | غير موافق (2) | غير موافق بشدة (1) | العبرة                                           |
|                   |                 |                |           |           |               |                    | إلى تأخيرات في جداول المشاريع التقنية.           |
| 1.28              | 3.40            | 20             | 35        | 20        | 15            | 10                 | 10.<br>تؤدي الحوادث الأمنية السيبرانية إلى زيادة |

|                   |                 |                |           |           |               |                    |                                                           |
|-------------------|-----------------|----------------|-----------|-----------|---------------|--------------------|-----------------------------------------------------------|
| الانحراف المعياري | المتوسط الحسابي | موافق بشدة (5) | موافق (4) | محايد (3) | غير موافق (2) | غير موافق بشدة (1) | العبارة                                                   |
|                   |                 |                |           |           |               |                    | في تكاليف المشاريع التقنية.                               |
| 1.22              | 3.60            | 25             | 37        | 18        | 13            | 7                  | 11. تؤثر التهديدات السيبرانية على جودة أو موثوقية الأنظمة |

|                   |                 |                |           |           |               |                    |                   |
|-------------------|-----------------|----------------|-----------|-----------|---------------|--------------------|-------------------|
| الانحراف المعياري | المتوسط الحسابي | موافق بشدة (5) | موافق (4) | محايد (3) | غير موافق (2) | غير موافق بشدة (1) | العبارة           |
|                   |                 |                |           |           |               |                    | التي يتم تطويرها. |

التحليل الأولي: على الرغم من أن متوسط التحديات المتكررة (العبارة 8) هو 2.95

(أقرب إلى المحايد/غير الموافق)، فإن المستجيبين يوافقون بقوة على أن الاختراقات

الأمنية تؤدي إلى تأخيرات (متوسط 3.62) وزيادة في التكاليف (متوسط 3.40) وتأثير

سلبي على الجودة (متوسط 3.60). هذا يشير إلى أن حتى لو لم تكن الهجمات متكررة

جداً، فإن تأثيرها عند وقوعها يكون كبيراً.

المحور الرابع: الوعي والتدريب في الأمن السيبراني

يقيس هذا المحور مستوى الوعي والتدريب لدى فرق العمل.

| العبارة                                                             | غير موافق بشدة (1) | غير موافق (2) | محايد (3) | موافق (4) | موافق بشدة (5) | المتوسط الحسابي | الانحراف المعياري |
|---------------------------------------------------------------------|--------------------|---------------|-----------|-----------|----------------|-----------------|-------------------|
| 12.<br>يتلقى فريق عمل المشروع تدريباً كافياً حول أفضل ممارسات الأمن | 12                 | 18            | 20        | 30        | 20             | 3.28            | 1.35              |

| العبارة                                                            | غير موافق بشدة (1) | غير موافق (2) | محايد (3) | موافق (4) | موافق بشدة (5) | المتوسط الحسابي | الانحراف المعياري |
|--------------------------------------------------------------------|--------------------|---------------|-----------|-----------|----------------|-----------------|-------------------|
| السيبراني .                                                        |                    |               |           |           |                |                 |                   |
| 13.<br>يوجد وعي عالٍ بأهمية الأمن السيبراني بين جميع أصحاب المصلحة | 8                  | 12            | 25        | 35        | 20             | 3.55            | 1.22              |

|                    |                      |           |             |                |                 |                   |                      |
|--------------------|----------------------|-----------|-------------|----------------|-----------------|-------------------|----------------------|
| غير موافق بشدة (1) | غير موافق ق بشدة (2) | محايد (3) | موافق ق (4) | موافق بشدة (5) | المتوسط الحسابي | الانحراف المعياري | العبارة              |
|                    |                      |           |             |                |                 |                   | في المشاريع التقنية. |

التحليل الأولي: يشير متوسط 3.28 للعبارة 12 إلى أن هناك حاجة محتملة لتعزيز

التدريب على الأمن السيبراني لفرق عمل المشاريع. ومع ذلك، يبدو أن هناك وعيًا أعلى

بأهمية الأمن السيبراني (متوسط 3.55) بين أصحاب المصلحة بشكل عام.

## النتائج

### 1. تكامل الأمن السيبراني في مراحل المشروع:

- أظهرت النتائج أن هناك مستوى جيد من دمج متطلبات الأمن السيبراني في مرحلة تخطيط المشاريع التقنية في القطاع الحكومي السعودي، بمتوسط حسابي مرتفع للعبارة ذات الصلة (3.85 من 5).
- ومع ذلك، تبين أن مشاركة متخصصي الأمن السيبراني في جميع مراحل دورة حياة المشروع التقني أقل فعالية مقارنة بمرحلة التخطيط (متوسط 3.40)، مما يشير إلى وجود فجوة في التكامل المستمر.
- أكدت النتائج على أهمية إجراء تقييمات دورية للمخاطر الأمنية السيبرانية خلال تنفيذ المشاريع، حيث كان المتوسط الحسابي لهذه العبارة جيداً (3.64).

### 2. الالتزام بمعايير الأمن السيبراني وتأثيره على الأداء:

- يوجد التزام معقول بالمعايير الوطنية والدولية للأمن السيبراني في المشاريع التقنية (متوسط 3.55).
- أبرزت النتائج أن الالتزام بمعايير الأمن السيبراني يؤثر بشكل إيجابي وملحوظ على جودة مخرجات المشاريع التقنية (متوسط 3.80).
- في المقابل، كان تأثير الالتزام بمعايير الأمن السيبراني على تسليم المشاريع في الوقت المحدد والالتزام بالميزانية المخصصة أقل وضوحاً (متوسط 3.35 للوقت و

3.20 للتكلفة)، مما قد يشير إلى تحديات في تحقيق التوازن بين المتطلبات

الأمنية وجدولة المشاريع وتكاليفها.

3. التحديات الأمنية السيبرانية وتأثيرها على الفعالية:

- على الرغم من أن المشاركين لم يشيروا إلى تكرار كبير للهجمات مثل التصيد الاحتيالي والبرمجيات الخبيثة (متوسط 2.95)، إلا أنهم أكدوا بشكل كبير على أن الاختراقات الأمنية السيبرانية تؤدي إلى تأخيرات في جداول المشاريع (متوسط 3.62).

- كما أشارت النتائج إلى أن الحوادث الأمنية السيبرانية تساهم في زيادة تكاليف المشاريع (متوسط 3.40).

- كذلك، كان هناك اتفاق على أن التهديدات السيبرانية تؤثر سلباً على جودة وموثوقية الأنظمة التي يتم تطويرها (متوسط 3.60).

4. الوعي والتدريب في الأمن السيبراني:

- تبين أن هناك وعياً جيداً بأهمية الأمن السيبراني بين جميع أصحاب المصلحة في المشاريع التقنية (متوسط 3.55).

- ومع ذلك، أظهرت النتائج أن مستوى التدريب الذي يتلقاه فريق عمل المشروع حول أفضل ممارسات الأمن السيبراني يحتاج إلى تعزيز (متوسط 3.28)، مما يشير إلى فجوة بين الوعي النظري والتطبيق العملي من خلال التدريب المتخصص.

## التوصيات

### 1. تعزيز التكامل الشامل للأمن السيبراني في دورة حياة المشروع:

- يجب التأكيد على ضرورة إشراك متخصصي الأمن السيبراني بشكل مكثف وفعال في جميع مراحل المشروع، وليس فقط في مرحلتي التخطيط والتنفيذ الأولي. يجب أن يكونوا جزءاً لا يتجزأ من فريق المشروع لضمان دمج المتطلبات الأمنية بشكل استباقي.
- تطوير إطار عمل واضح ومعيارى لتكامل الأمن السيبراني في كل مرحلة من مراحل دورة حياة المشروع (بدء، تخطيط، تنفيذ، مراقبة وتحكم، إغلاق).

### 2. الموازنة بين متطلبات الأمن وقيود المشروع (الوقت والتكلفة):

- إجراء تحليل دقيق للتكلفة والفوائد (Cost-Benefit Analysis) لتدابير الأمن السيبراني لضمان أنها لا تسبب تجاوزات غير مبررة في الميزانية أو تأخيرات في الجدول الزمني.

- تبني منهجيات تطوير رشيقة (Agile Methodologies) مع دمج الأمن السبراني بشكل مستمر (DevSecOps) لتقليل تأثير التغييرات الأمنية المتأخرة على الوقت والتكلفة.

### 3. الاستثمار في برامج التدريب المتخصصة ورفع الكفاءة:

- وضع برامج تدريب مكثفة ومستمرة لفرق عمل المشاريع التقنية، لا سيما مدراء المشاريع والمهندسين والمطورين، حول أحدث ممارسات وتحديات الأمن السبراني.
- تضمين السيناريوهات العملية والمحاكاة في التدريب لتعزيز الاستجابة للحوادث الأمنية.
- تشجيع الحصول على الشهادات الاحترافية في الأمن السبراني وإدارة المشاريع الآمنة.

### 4. تطوير آليات استباقية لإدارة التحديات الأمنية:

- تعزيز ثقافة الأمن السبراني من خلال حملات توعية مستمرة لجميع الموظفين، مع التركيز على التهديدات الشائعة مثل التصيد الاحتيالي والهندسة الاجتماعية.
- الاستثمار في أدوات وتقنيات الكشف المبكر عن التهديدات والاستجابة للحوادث لتقليل الأثر السلبي للاختراقات على سير المشاريع.

◦ تطوير خطط استمرارية الأعمال والتعافي من الكوارث السيبرانية لضمان

استمرارية المشاريع حتى في حال وقوع حوادث كبيرة.

5. تفعيل دور قيادات الأمن السيبراني في صنع القرار:

◦ منح قيادات الأمن السيبراني سلطة كافية في اتخاذ القرارات المتعلقة

بالمشاريع التقنية، خاصة تلك التي تحمل مخاطر أمنية عالية.

◦ إنشاء لجان مشتركة تضم ممثلين عن إدارة المشاريع والأمن السيبراني

لمراجعة وتقييم المشاريع بشكل دوري.

1. عبد الرازق، أمين أبو شعر. (1997). العينات وتطبيقاتها في البحوث الاجتماعية. معهد الإدارة العامة.
2. الحبيب، ماجد. (2022). درجة الوعي بالأمن السيبراني لدى طلاب وطالبات الدراسات العليا بكلية التربية بجامعة الإمام محمد بن سعود الإسلامية وسبل تعزيزه من وجهة نظرهم. مجلة العلوم التربوية، 30(1).
3. الحداد، نبيلة محمد أحمد. (2022). متطلبات تحقيق الأمن السيبراني في المكتبات الجامعية اليمنية: دراسة حالة. مجلة جامعة البيضاء، 4(2)، 703-715.
4. حمامي، عادل. (2022). الآليات القانونية لحماية الأمن السيبراني. في الملتقى الدولي عن بعد حول الأمن السيبراني والتحديات المعاصرة. جامعة غرداية، الجزائر.
5. زقوت، نشوة. (2022). مدى وعي أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبراني في ظل التحول الرقمي دراسة تطبيقية بجامعة الزاوية. المجلة الدولية للعلوم والتقنية، كلية تقنية المعلومات، جامعة الزاوية. (1-14).
6. زروقة، إسماعيل. (2019). الفضاء السيبراني والتحول في مفاهيم القوة والصراع. مجلة العلوم القانونية والسياسية، 10(1)، 10-17.

7. السمحان، منى عبد الله. (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. مجلة كلية التربية جامعة المنصورة، (111).
8. شركة ريناد المجد لتقنية المعلومات. (2023). ضوابط الأمن السيبراني للبيانات. تم الاسترجاع في 5 مارس 2023، من [/https://www.mg-sa.com](https://www.mg-sa.com)
9. صائغ، وفاء. (2018). وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياجاتهم الأمنية من الجرائم الإلكترونية. المجلة العربية للعلوم الاجتماعية، المؤسسة العربية للاستشارات العلمية، (29).
10. الجنفاوي، خالد مخلف. (2021). التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت. المجلة العربية للآداب والدراسات الإنسانية، (19)، 75-123.
11. الجوهري، هيثم. (2023). دليل الالتزام بضوابط ومتطلبات الأمن السيبراني في المملكة العربية السعودية. شبكة بي دبليو سي.
12. القحطاني، نورة بنت ناصر. (2019). مدى توفر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي من وجهة نظرهم. مجلة شئون اجتماعية، جمعية الاجتماعيين في الشارقة، 36(144)، 85-144.

13. فرج، علياء عمر. (2022). دواعي تعزيز ثقافة الأمن السيبراني في ظل

التحول الرقمي: جامعة الأمير سطام بن عبد العزيز نموذجًا. *المجلة التربوية*،

جامعة سوهاج، 94.

14. الهزاني، نورة بنت ناصر. (2021). المعرفة والشبكات الاجتماعية. دار

تكوين.

15. الهيئة الوطنية للأمن السيبراني. (2022). وثيقة ضوابط الأمن السيبراني

للبيانات. الهيئة الوطنية للأمن السيبراني.

16. الهيئة الوطنية للأمن السيبراني. (2023). نبذة عن الهيئة الوطنية للأمن

السيبراني. تم الاسترجاع في 6 مارس 2023، من

<https://nca.gov.sa/about>

## ملخص الدراسة

هدفت هذه الدراسة إلى تحديد وتحليل أثر الأمن السيبراني على فعالية إدارة المشاريع

التقنية في القطاع الحكومي بالمملكة العربية السعودية. جاءت هذه الأهمية في ظل

التوسع الرقمي الذي تشهده المملكة ورؤية 2030، والتي تضع الأمن السيبراني كركيزة

أساسية لنجاح المشاريع التقنية الحكومية.

تضمنت مشكلة الدراسة الرئيسية سؤالاً حول مدى تأثير الأمن السيبراني على فعالية إدارة

المشاريع، وتفرعت منها أسئلة حول تكامل الأمن السيبراني، تأثيره على مؤشرات الأداء

(الوقت، التكلفة، الجودة)، أبرز التحديات الأمنية، ومستوى الوعي والتدريب.

لتحقيق أهدافها، اعتمدت الدراسة على المنهج الوصفي التحليلي، وتم استخدام الاستبانة

كأداة رئيسية لجمع البيانات من مجتمع الدراسة المتمثل في العاملين بإدارة المشاريع التقنية

والأمن السيبراني في القطاع الحكومي السعودي. تم تحليل 100 استجابة باستخدام

الإحصاء الوصفي.

أظهرت النتائج أن هناك وعياً جيداً بأهمية دمج الأمن السيبراني في تخطيط المشاريع،

وأن الالتزام بمعايير الأمن السيبراني يؤثر إيجاباً على جودة مخرجات المشاريع. ومع ذلك،

كشفت النتائج عن فجوة في التكامل المستمر للأمن السيبراني خلال مراحل المشروع، وأن

التحديات الأمنية السيبرانية (حتى لو لم تكن متكررة) تؤدي إلى تأخيرات وزيادات في

التكلفة وتأثير سلبي على جودة المشاريع. كما أشارت النتائج إلى الحاجة لتعزيز برامج التدريب على الأمن السيبراني لفرق عمل المشاريع.

بناءً على هذه النتائج، أوصت الدراسة بتعزيز التكامل الشامل للأمن السيبراني في جميع مراحل دورة حياة المشروع، والموازنة بين متطلبات الأمن وقيود المشروع (الوقت والتكلفة)، والاستثمار في برامج التدريب المتخصصة ورفع الكفاءة، وتطوير آليات استباقية لإدارة التحديات الأمنية، وأخيراً تفعيل دور قيادات الأمن السيبراني في صنع القرار، بهدف تحقيق مشاريع تقنية أكثر فعالية وأماناً في القطاع الحكومي بالمملكة.

استبيان

الهدف العام للاستبيان:

يهدف هذا الاستبيان إلى جمع البيانات حول مدى تأثير ممارسات وتحديات الأمن السيبراني على فعالية إدارة المشاريع التقنية في الجهات الحكومية بالمملكة العربية السعودية، وذلك لتحديد العلاقة بينهما واقتراح توصيات لتحسين الأداء.

تعليمات:

يرجى قراءة كل عبارة بعناية واختيار الإجابة التي تعبر عن رأيك أو واقع الحال بأكبر دقة، باستخدام المقياس التالي:

(1) غير موافق بشدة (2) غير موافق (3) محايد (4) موافق (5) موافق بشدة

المحور الأول: تكامل الأمن السيبراني في مراحل المشروع

4. يتم دمج متطلبات الأمن السيبراني في مرحلة تخطيط المشاريع التقنية لدينا.

(1) (2) (3) (4) (5)

5. يشارك متخصصو الأمن السيبراني بفعالية في جميع مراحل دورة حياة المشروع التقني.

(1) (2) (3) (4) (5)

6. يتم إجراء تقييمات للمخاطر الأمنية السيبرانية بشكل دوري خلال تنفيذ المشاريع.

(1) (2) (3) (4) (5)

المحور الثاني: الالتزام بمعايير الأمن السيبراني وتأثيره على الأداء

8. تلتزم مشاريعنا التقنية بالمعايير الوطنية والدولية للأمن السيبراني (مثل ISO

27001، CIS Controls).

(1) (2) (3) (4) (5)

9. الالتزام بمعايير الأمن السيبراني يساهم في تسليم المشاريع التقنية في الوقت

المحدد.

(1) (2) (3) (4) (5)

10. الالتزام بمعايير الأمن السيبراني يساعد في الالتزام بالميزانية المخصصة

للمشاريع التقنية.

(1) (2) (3) (4) (5)

11. الالتزام بمعايير الأمن السيبراني يرفع من جودة مخرجات المشاريع التقنية.

(1) (2) (3) (4) (5)

### المحور الثالث: التحديات الأمنية السيبرانية وتأثيرها على الفعالية

12. نواجه تحديات متكررة تتعلق بهجمات التصيد الاحتيالي أو البرمجيات

الخبیثة في مشاريعنا.

(1) (2) (3) (4) (5)

13. تؤدي الاختراقات الأمنية السيبرانية إلى تأخيرات في جداول المشاريع

التقنية.

(1) (2) (3) (4) (5)

14. تؤدي الحوادث الأمنية السيبرانية إلى زيادة في تكاليف المشاريع التقنية.

(1) (2) (3) (4) (5)

15. تؤثر التهديدات السيبرانية على جودة أو موثوقية الأنظمة التي يتم تطويرها.

(1) (2) (3) (4) (5)

### المحور الرابع: الوعي والتدريب في الأمن السيبراني

14. يتلقى فريق عمل المشروع تدريباً كافياً حول أفضل ممارسات الأمن

السيبراني.

(1) (2) (3) (4) (5)

15. يوجد وعي عالٍ بأهمية الأمن السيبراني بين جميع أصحاب المصلحة في

المشاريع التقنية.

(1) (2) (3) (4) (5)

Midwestern University,  
College of Management,  
Department of Business  
Administration,  
Master of Business Administration (MBA)



The Impact of Cybersecurity on the Effectiveness of Technical  
Project Management: An Applied Study on the Government Sector  
in the Kingdom of Saudi Arabia

Prepared by Mansour Daghfaq Alenezi

Supervised by Dr. Al Faisal Abdelhamid Muhammad

Dr. Fayez Ali Jarad

Academic Year 2025