

جامعة ميدأوشن

كلية الإدارة

قسم / تخصص ماجستير إدارة مخاطر



عنوان البحث

أثر الهجمات السيبرانية على استمرارية برامج المشاريع في المؤسسات الكبرى – دراسة تطبيقية على إحدى الجهات السعودية

"Assessing the Impact of Cyber Attacks on the Continuity of Program Management in Major Organizations: An Empirical Study on a Saudi Organization"

إعداد الطالب/ توفيق ميشيل المشرقي

الرقم الجامعي / 241002346

إشراف/

د. فايز جراد

د. الفیصل عبد الحمید

العام الدراسي:

2025

مقدمة:

تشهد المؤسسات الكبرى حول العالم تحولات رقمية متسارعة، زاد معها الاعتماد على التقنيات المتقدمة في تنفيذ برامج المشاريع. هذا التوسع الرقمي صاحبه تصاعد في حجم وخطورة الهجمات السيبرانية، ما فرض تحديات جديدة أمام مديري المشاريع ومسؤولي استمرارية الأعمال.

تُعرّف الهجمات السيبرانية بأنها: "أي نشاط ضار يُنفذ من خلال أنظمة الحاسوب بهدف اختراق، أو تعطيل أو سرقة أو تشويه معلومات أو أنظمة رقمية (NIST, 2022)".

أما برامج المشاريع فهي: "مجموعة من المشاريع ذات العلاقة التي تُدار بطريقة منسقة لتحقيق منافع لا يمكن تحقيقها بإدارتها بشكل منفصل. (PMI, 2021)".

ويُقصد بـ استمرارية البرامج: قدرة المؤسسات على مواصلة تنفيذ تلك البرامج وتحقيق أهدافها رغم الأزمات والاضطرابات.

في هذا السياق، تبرز أهمية التحقق من أثر الهجمات السيبرانية على استمرارية برامج المشاريع في المؤسسات الكبرى، خاصةً أن تعطل أي مكون رقمي حرج قد يؤدي إلى توقف كلي أو جزئي يهدد فعالية الأداء المؤسسي ككل.

مشكلة الدراسة:

مع تصاعد الهجمات السيبرانية، تواجه المؤسسات الكبرى تهديدًا حقيقيًا لاستمرارية برامجها الحيوية. حيث تؤدي هجمات مثل حجب الخدمة (DDoS) أو برامج الفدية (Ransomware) إلى تعطيل الأنظمة، تسرب البيانات، أو تدمير البنية التحتية الرقمية، مما ينعكس بشكل مباشر على برامج المشاريع من حيث التأخير، زيادة التكاليف، وتدهور جودة التنفيذ.

رغم وجود العديد من الدراسات التي تناولت أمن المعلومات أو استمرارية الأعمال، إلا أن القليل منها ركّز على الربط المباشر بين الهجمات السيبرانية واستمرارية برامج المشاريع، مما يخلق فجوة بحثية تحتاج إلى معالجة دقيقة لفهم العلاقة وتأثيرها الواقعي.

أهمية الدراسة:

تبرز أهمية هذه الدراسة من جوانب متعددة:

1. أهمية علمية: تسهم الدراسة في سد فجوة معرفية تتعلق بتقاطع ثلاثة مجالات حرجية: الأمن السيبراني، إدارة المشاريع، واستمرارية الأعمال، وهو تقاطع لم يُسلط عليه الضوء بشكل كافٍ في الأدبيات الحديثة.
2. أهمية تطبيقية: تساعد نتائج الدراسة في تعزيز الوعي المؤسسي حول مدى خطورة التهديدات السيبرانية على البرامج طويلة الأمد، وتقديم توصيات لتحسين خطط الاستجابة وحماية الاستثمارات التقنية.
3. أهمية وطنية: تأتي هذه الدراسة تماشيًا مع رؤية المملكة 2030 في مجال التحول الرقمي، مما يجعل من الضروري استكشاف المخاطر المرتبطة بهذا التحول على مستوى التنفيذ المؤسسي للبرامج.

أهداف الدراسة:

- تحليل تأثير الهجمات السيبرانية على برامج المشاريع.
- تحديد أبرز نقاط الضعف في استمرارية البرامج التقنية.
- تقديم إطار عملي لإدارة المخاطر السيبرانية في سياق المشاريع.

تساؤلات الدراسة

- ما أنواع الهجمات السيبرانية الأكثر تأثيرًا على برامج المشاريع؟
- كيف تؤثر هذه الهجمات على استمرارية البرامج من حيث الوقت والجودة؟
- ما التدابير الوقائية الممكنة لضمان استمرارية البرامج؟

فروض الدراسة:

- توجد علاقة ذات دلالة إحصائية بين تعرض المؤسسة لهجمات سيبرانية وتعرض استمرارية برامج المشاريع.
- يختلف تأثير الهجمات السيبرانية على البرامج باختلاف نوع القطاع (حكومي/خاص)، أو مستوى جاهزية المؤسسة من حيث الأمن السيبراني.
- تساهم خطط استمرارية الأعمال وخطط الاستجابة للحوادث في تقليل الأثر السلبي للهجمات على تنفيذ البرامج.

الدراسات السابقة:

تُظهر الأدبيات الأكاديمية الحديثة اهتمامًا متزايدًا بتأثير الهجمات السيبرانية على المؤسسات، وخاصة فيما يتعلق بالأمن المعلوماتي واستمرارية الأعمال. ركزت بعض الدراسات على الخسائر الاقتصادية الناتجة عن تلك الهجمات، مثل دراسة (IBM, 2023) التي تناولت متوسط تكلفة خرق البيانات في القطاعات الحيوية، ودراسة (ENISA, 2022) التي حللت أثر الهجمات على استقرار الخدمات الحكومية.

ومع ذلك، فإن معظم تلك الدراسات لم تتناول بوضوح تأثير الهجمات السيبرانية على استمرارية برامج المشاريع كمظلة تنفيذية تجمع عدّة مشاريع مترابطة، مما يبرز الحاجة لإجراء دراسة تدمج بين البعدين الأمني والإداري للمؤسسات الكبرى.

المنطلقات النظرية للدراسة:

- تركز هذه الدراسة على مجموعة من المفاهيم النظرية والنماذج المعتمدة عالمياً، من أبرزها:
 - إطار إدارة مخاطر الأمن السيبراني: (NIST SP 800-30) والذي يقدم خطوات منظمة لتقييم وتحليل المخاطر الرقمية.
 - نموذج استمرارية الأعمال: (ISO 22301) والذي يشرح كيفية إعداد وتنفيذ خطط الاستجابة والتعافي المؤسسي.
 - مفاهيم إدارة البرامج وفق PMI: لفهم كيف تؤثر المخاطر الخارجية (مثل الهجمات السيبرانية) على أداء البرنامج بأكمله.
- يتم توظيف هذه الأطر النظرية لفهم العلاقة المعقدة بين التهديدات الرقمية والقدرة المؤسسية على تنفيذ البرامج الاستراتيجية.

المنهجية وطرق البحث:

نظرًا لطبيعة الموضوع وضيق الوقت، تعتمد هذه الدراسة على المنهج التحليلي بالاعتماد على البيانات الثانوية، حيث يتم تحليل محتوى عدد من:

- التقارير الرسمية: مثل تقارير Kaspersky ، IBM Security ، Cisco ، تقارير الهيئة الوطنية للأمن السيبراني.

- دراسات حالة منشورة: لحوادث اختراق أثّرت على مشاريع كبرى مثل SolarWinds أو Colonial Pipeline.

- الأدبيات الأكاديمية المحكمة: لتأطير المفاهيم النظرية وتحديد أوجه العلاقة.

يتيح هذا الأسلوب فهمًا أعمق للتأثير الواقعي للهجمات السيبرانية دون الحاجة إلى تنفيذ أدوات جمع بيانات ميدانية مثل الاستبانات أو المقابلات.

أدوات الدراسة:

- مراجعة منهجية للتقارير التقنية الصادرة عن شركات الأمن السيبراني والهيئات التنظيمية.
- تحليل محتوى لحالات اختراق منشورة. (Case Studies)
- مراجعة الدراسات الأكاديمية المحكمة ذات الصلة.

حدود الدراسة:

- موضوعية: تركز على أثر الهجمات السيبرانية على استمرارية برامج المشاريع.
- مكانية: تقتصر على مؤسسات كبرى ضمن المملكة العربية السعودية.
- زمانية: تتناول البيانات والحالات التي وقعت خلال الأعوام 2020-2024.
- منهجية: تعتمد فقط على تحليل بيانات ثانوية دون جمع بيانات ميدانية.

المراجع:

National Institute of Standards and Technology (NIST). (2022). SP 800-30: Guide for Conducting Risk Assessments.

Project Management Institute (PMI). (2021). Standard for Program Management – 4th Edition.

ISO/IEC 22301:2019 – Business continuity management systems.

IBM Security. (2023). Cost of a Data Breach Report.

ENISA Threat Landscape Report.(2022)

دراسات عربية منشورة في مجلات جامعية متخصصة في الأمن السيبراني وإدارة المشاريع.