

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:

كما يسعى البحث إلى تقديم إطار تحليلي يدعم المؤسسات في تعزيز جاهزيتها السيبرانية وضمان استدامة برامجها الحيوية. وفي هذا السياق، يهدف هذا البحث إلى تحليل أثر الهجمات السيبرانية على استمرارية برامج المشاريع في المؤسسات الكبرى، من خلال دراسة طبيعة التهديدات الرقمية، وتحديد مواطن الضعف المرتبطة بالبرامج، وتقييم الانعكاسات التشغيلية لهذه الهجمات. وتعرف الهجمات السيبرانية بأنها أنشطة ضارة تستهدف الأنظمة المعلوماتية بقصد الوصول غير المشروع أو إيقاف الخدمات أو الإضرار بالبيانات، بينما تشير استمرارية البرامج إلى قدرة المؤسسة على مواصلة تنفيذ برامجها رغم الظروف الطارئة. وفي ظل هذا الاعتماد المتنامي على الأنظمة الرقمية، تزايدت الهجمات السيبرانية بوصفها أحد أبرز المخاطر المؤسسية، نظرًا لقدرتها على تعطيل الأنظمة الحساسة، والإضرار بسلامة البيانات، وإحداث اضطرابات قد تطال البرامج الاستراتيجية. تشهد المؤسسات الكبرى تحولًا رقميًا متسارعًا جعل من البنية التكنولوجية عنصرًا جوهريًا في إدارة برامج المشاريع، التي تُعد إطارًا تنظيميًا ينسق بين مجموعة من المشاريع ذات العلاقة لتحقيق منافع استراتيجية مشتركة.

مشكلة الدراسة:

وانطلاقًا من ذلك، يسعى هذا البحث إلى معالجة المشكلة من خلال تحليل أنواع الهجمات الأكثر تأثيرًا، وتحديد مواطن الضعف في بيئة البرامج، وشرح الآثار التشغيلية والتنظيمية للاختراقات على سير البرنامج ومخرجاته، إلى جانب تقديم تصور تحليلي يدعم المؤسسات في تعزيز جاهزيتها وضمان استدامة برامجها.

وفي السياق السعودي، يزداد حجم المشكلة نظرًا لتسارع التحول الرقمي وارتفاع مستوى الاستهداف السيبراني للقطاعات الحيوية، الأمر الذي يبرز الحاجة إلى دراسة منهجية تُقيّم كيفية تأثير استمرارية برامج المشاريع بهذه الهجمات.

وتتمثل المشكلة الرئيسة في أن العديد من المؤسسات تركز على حماية الأنظمة التشغيلية اليومية، بينما تُهمل تحليل أثر تلك الهجمات على مستوى برامج المشاريع التي تعتمد بشكل واسع على الأنظمة الرقمية والمنصات التقنية، مما يؤدي إلى تعثر البرامج أو تأخرها أو ارتفاع تكاليفها دون ربط واضح بهذه التهديدات.

على الرغم من اعتماد المؤسسات الكبرى على برامج المشاريع بوصفها إطارًا تنفيذيًا يسهم في تحقيق الأهداف الاستراتيجية، إلا أن تزايد الهجمات السيبرانية خلال السنوات الأخيرة أصبح يشكل تحديًا مباشرًا لسلامة هذه البرامج واستمراريته.

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:

1. تقديم إطار تحليلي أو توصيات عملية لتعزيز استمرارية برامج المشاريع وحماية مكوناتها الحيوية.
2. استعراض أفضل الممارسات والأطر المرجعية التي تدعم جاهزية المؤسسات في مواجهة المخاطر السيبرانية.
3. تقييم تأثير الهجمات السيبرانية على عناصر استمرارية البرامج مثل الوقت والتكلفة والجودة والموارد.
4. تحليل نقاط الضعف التقنية والإدارية التي تجعل برامج المشاريع عرضة للتأثر بالتهديدات الرقمية.
5. تحديد أنواع الهجمات السيبرانية الأكثر تأثيرًا على برامج المشاريع في المؤسسات الكبرى.

تساؤلات الدراسة:

1. ما الممارسات أو الأطر المرجعية التي يمكن أن تعزز قدرة المؤسسات على حماية برامجها وضمان استدامتها في ظل التهديدات الرقمية؟
2. إلى أي مدى تسهم خطط استمرارية الأعمال وخطط الاستجابة للحوادث في الحد من تأثير الهجمات السيبرانية على برامج المشاريع؟
3. كيف تؤثر الهجمات السيبرانية على عناصر استمرارية البرامج مثل الوقت والتكلفة والجودة وإدارة الموارد؟
4. ما أبرز نقاط الضعف التقنية والتنظيمية التي تجعل برامج المشاريع عرضة للتأثر بالتهديدات السيبرانية؟
5. ما أنواع الهجمات السيبرانية الأكثر شيوعًا وتأثيرًا على برامج المشاريع في المؤسسات الكبرى؟

فروض الدراسة:

1. يسهم تطبيق الأطر المرجعية والممارسات الأمنية المعتمدة في رفع جاهزية البرامج وتقليل أثر الهجمات السيبرانية على استمراريته.
2. تساهم خطط استمرارية الأعمال وخطط الاستجابة للحوادث في الحد من تأثير الهجمات السيبرانية على سير برامج المشاريع.
3. للهجمات السيبرانية تأثير مباشر على عناصر استمرارية البرامج مثل الوقت والتكلفة والجودة والموارد.
4. تؤدي نقاط الضعف التقنية والتنظيمية داخل بيئة البرامج إلى زيادة احتمالية تأثرها بالهجمات السيبرانية.
5. يختلف تأثير الهجمات السيبرانية على برامج المشاريع باختلاف طبيعة ونوع الهجوم.

الدراسات السابقة:

من خلال تحليل هذه الدراسات تتضح فجوة بحثية في مستوى برامج المشاريع.

تشير تقارير إلى ضرورة رفع جاهزية القطاعات الحيوية NCA.

أولاً: دراسات عربية وسعودية ركزت على الأمن السيبراني واستمرارية الأعمال.

أكدت دراسات على أهمية دمج الأمن السيبراني ضمن حوكمة البرامج PMI.

ثانياً: دراسات تناولت إدارة البرامج وتأثرها بالمخاطر التقنية.

كما أشارت إلى تعقد الهجمات وتأثيرها على سلاسل التوريد التقنية (ENISA 2022).

بينت دراسة ارتفاع تكاليف الاختراق وتأثيرها المباشر على العمليات (IBM 2023).

ثالثاً: دراسات دولية حديثة تناولت تطور التهديدات السيبرانية وأثرها على البنى التحتية.

تمثل الدراسات السابقة الأساس العلمي لفهم العلاقة بين الهجمات السيبرانية واستمرارية برامج المشاريع.

تظهر الفجوة في محدودية الدراسات التي عالجت أثر الهجمات على استمرارية برامج المشاريع تحدياً.

المنطلقات النظرية للدراسة:

تتوسط العلاقة جاهزية الأمن السيبراني وخطط الاستجابة للحوادث ونضج إدارة البرامج.

تؤدي الهجمات السيبرانية إلى تعطّل الأنظمة والمنصات المشتركة مما يؤثر على الوقت والتكلفة والجودة واستمرارية المنافع.

المتغير المستقل: الهجمات السيبرانية.

المتغير التابع: استمرارية برامج المشاريع .

العلاقة بين المتغيرات:

تشمل عناصرها تقييم المخاطر، خطط الاستجابة للحوادث، خطط التعافي، BIA تحليل تأثير الأعمال.

تُعرّف استمرارية الأعمال بأنها قدرة المؤسسة على الاستجابة للاضطرابات واستعادة الأنشطة الحيوية إلى المستوى المقبول خلال مدة ISO 22301 وفق زمنية محددة.

استمرارية الأعمال:

تعتبر برامج المشاريع أكثر حساسية للمخاطر التقنية نظرًا لاعتمادها الكبير على الأنظمة والمنصات المشتركة.

يُعرّف البرنامج بأنه مجموعة من المشاريع ذات العلاقة التي تُدار بطريقة منسقة لتحقيق منافع مشتركة. تشمل مكونات البرنامج: إدارة المنافع، PMI، وفقًا ل إدارة أصحاب المصلحة، إدارة المخاطر، والحوكمة.

إدارة برامج المشاريع:

برامج الفدية، الهجمات عبر سلاسل التوريد، والهجمات الداخلية، (DDoS) تشمل الهجمات السيبرانية الشائعة: هجمات حجب الخدمة.

يُعرّف الأمن السيبراني بأنه مجموعة من العمليات والتقنيات والممارسات المصممة لحماية الأنظمة الرقمية والشبكات والبيانات من الهجمات أو الوصول غير يشمل الأمن السيبراني ثلاث ركائز أساسية: السرية، السلامة، التوافر. (NIST, 2022) المصرّح به.

المخطط المفاهيمي للدراسة:

تشترك هذه الهجمات في قدرتها على تعطيل الأنظمة المركزية، مما يجعل برامج المشاريع عرضة لتعثر كبير.

تستغل ثغرات لم يتم إصلاحها بعد (Zero-Day) هجمات اليوم الصفرى

يقوم بها مستخدم ذو صلاحيات عالية (Insider Threats) الهجمات الداخلية.

SolarWinds تُعد من أخطر الأنواع، مثل حادثة (Supply Chain Attacks) هجمات سلسلة التوريد.

تعتمد على إغراق الخادم بطلبات هائلة تؤدي لوقف الأنظمة (DDoS) هجمات حجب الخدمة.

تؤثر هذه الهجمات على برامج المشاريع من خلال توقف تدفق البيانات بين المشاريع.

المنهجية وطرق البحث:

خطوات التحليل تشمل: جمع الدراسات، المقارنة المرجعية، تحليل الأنماط.

يمثل هذا المنهج الأنسب لطبيعة البحث لأنه لا يتطلب جمع بيانات أولية.

تشمل منهجية العمل تحليل محتوى للدراسات وحالات اختراق فعلية.

يستند إلى تحليل البيانات الثانوية من التقارير والدراسات.

يعتمد البحث على المنهج الوصفي التحليلي.

كما يساعد المنهج الوصفي التحليلي في استخلاص النتائج وتقديم إطار تحليلي لدعم المؤسسات في تعزيز جاهزيتها أمام التهديدات السيبرانية.

ويتم تطبيق المنهج عبر جمع البيانات الثانوية، وتحليل محتوى التقارير، وإجراء المقارنة المرجعية بين الممارسات العالمية والمحلية.

تبرز أهمية هذا المنهج في قدرته على الكشف عن أنماط التأثير بين المتغيرات وتفسير العلاقة بين الهجمات السيبرانية واستمرارية البرامج.

يستند البحث إلى مراجعة الأدبيات والدراسات السابقة والتقارير الدولية والوطنية بهدف وصف الهجمات السيبرانية وتحليل أثرها على البرامج.

وقد تم اختيار هذا المنهج نظراً لملاءمته لطبيعة موضوع البحث الذي يتطلب تحليل بيانات ثانوية تتعلق بالهجمات السيبرانية واستمرارية برامج المشاريع.

يعتمد هذا البحث على المنهج الوصفي التحليلي، وهو منهج يقوم على وصف الظاهرة المدروسة وتحليل مكوناتها واستنتاج العلاقات بينها.

المنهجية وطرق البحث:

يهدف استنتاج أنماط التأثير دراسة حالات اختراق عالمية مثل Colonial Pipeline و SolarWinds

تحليل محتوى التقارير الدولية والوطنية مثل NCA و ENISA و NIST.

تعتمد الدراسة على أدوات رئيسية لجمع وتحليل البيانات:

أولاً: المراجعة المنهجية للأدبيات عبر تحليل الدراسات المحكمة المرتبطة بالأمن السيبراني واستمرارية البرامج.

تم تحليل الدراسات الأكاديمية المحكمة العربية والأجنبية لتحديد العلاقة بين الأمن السيبراني واستمرارية برامج المشاريع وتحديد الفجوة البحثية.

ثانياً: تحليل محتوى الدراسات السابقة.

يهدف، SAMA و DGA و NCA إضافة إلى السياسات الوطنية الصادرة عن، NIST و ENISA و IBM شمل تحليل التقارير الدولية مثل

دراسة طبيعة الهجمات السيبرانية وآثارها.

حدود الدراسة:

يوصي البحث بدمج الأمن السيبراني ضمن حوكمة البرامج وتعزيز خطط الاستمرارية.

كما أن جاهزية الأمن السيبراني تمثل عاملاً وسيطاً مهماً في تخفيف التأثير.

بيّن التحليل أن الهجمات تؤثر على الوقت والتكلفة والجودة وتدفق المنافع.

خلص البحث إلى أن الهجمات السيبرانية تمثل خطراً مباشراً على استمرارية البرامج.

الحدود المنهجية: تستند إلى بيانات ثانوية دون جمع بيانات ميدانية.

الحدود الزمانية: تعتمد على بيانات ودراسات بين 2020-2024.

الحدود المكانية: تشمل مؤسسات كبرى داخل المملكة العربية السعودية.

الحدود الموضوعية: تركز الدراسة على أثر الهجمات السيبرانية على استمرارية برامج المشاريع دون التطرق للمشاريع الفردية.

- Al-Somali, T. (2024). Cybersecurity capabilities and organizational resilience in service firms Sustainability, 16(3), 1–19
- European Union Agency for Cybersecurity. (2022). ENISA threat landscape 2022
- Harake, N. (2025). Integrating cybersecurity into project management practices. International Journal of Project Management, 43(2), 115–129
- IBM Security. (2023). Cost of a data breach report 2023
- International Organization for Standardization. (2019). ISO 22301:2019 security and resilience – business continuity management systems – requirements
- National Institute of Standards and Technology. (2022). SP 800–30: Guide for conducting risk assessments
- National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1)
- Project Management Institute. (2021). The standard for program management (4th ed.)
- Saudi National Cybersecurity Authority. (2022). Cybersecurity controls for business continuity and disaster recovery
- Saudi Central Bank. (2021). Business continuity management framework for the financial sector
- Ahmad, A., Maynard, S. B., & Desouza, K. (2021). Information security strategies: Towards an integrated framework. Computers & Security, 103, 102–118
- Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cybersecurity awareness campaigns: Why do they fail? Computers & Security, 87, 101–115
- Saleh, A. & Alhabshi, S. (2020). Cybersecurity resilience in Gulf-region enterprises. Journal of Information Security, 9(4), 215–229
- AlHogail, A. (2018). Improving cybersecurity culture: A framework for organizations. International Journal of Advanced Computer Science, 9(1), 93–103