المجلة الدولية لنشر البحوث والدراسات
International Journal of Research and Studies Publishing
ISSN: 2709-7064
المجلد 7 - الإصدار 81
تاريخ النشر: 20 يوليو 2026 م

مستوى تكامل الأمن الفيزيائي والرقمي وعلاقة الأمن السيبراني بممارسات الامتثال الأمني بالمنشآت الصناعية السعودية في ضوء رؤية المملكة العربية السعودية 2030

The Level of Integration of Physical and Digital Security and the Relationship of Cybersecurity to Security Compliance Practices in Saudi Industrial Facilities in Light of the Kingdom of Saudi Arabia's Vision 2030

إعداد الباحث/ سلطان سعد محمد الحميد

باحث دكتوراه في إدارة الأعمال، جامعة ميد أوشن، الإمارات العربية المتحدة

الملخص:

هدفت الدراسة إلى التعرف على مستوى تكامل الأمن الفيزيائي والرقمي، والكشف عن العلاقة بين وجود قسم مختص بالأمن السيبراني ومستوى الامتثال الأمني في المنشآت الصناعية السعودية، وتفسير النتائج في ضوء رؤية المملكة العربية السعودية 2030. واعتمدت الدراسة المنهج الوصفي التحليلي، واستخدمت الاستبانة أداةً لجمع البيانات من عينة بلغت 215 مشاركًا، وتم تحليل البيانات باستخدام المتوسطات الحسابية والانحرافات المعيارية، إلى جانب اختبار كاي تربيع (Pearson Chi-Square) للكشف عن العلاقة بين المتغيرات، ومعامل Cramer's V لتحديد قوة العلاقة. وأظهرت النتائج أن مستوى ممارسات تكامل الأمن الفيزيائي والرقمي جاء بوجه عام ضمن المستوى المتوسط، بمتوسط وصفي بلغ نحو (2.83)، كما جاءت ممارسات الامتثال الأمني ضمن المستوى المتوسط بمتوسط بلغ نحو (2.85). وأفاد 47.4% من أفراد العينة بوجود قسم مختص بالأمن السيبراني في منشآتهم، مقابل 52.6% أفادوا بعدم وجوده. كما بينت نتائج اختبار كاي تربيع عدم وجود علاقة ذات دلالة إحصائية بين وجود قسم مختص بالأمن السيبراني ومستوى الامتثال الأمني ($\chi 2$ =1.094، p=0.895)، مع ضعف شديد في قوة العلاقة وفق معامل Cramer's V. وأظهرت البنود المرتبطة بالتحول الرقمي والجاهزية والحوكمة والأمن السيبراني الوطني والتنافسية الصناعية مستوى متوسطًا بمتوسط وصفي بلغ نحو (2.74)، بما يعكس أهمية مواصلة تطوير ممارسات التكامل في ضوء توجهات رؤية المملكة 2030. وأوصت الدراسة بتعزيز التكامل التقني والتنظيمي، وتطوير السياسات وآليات الامتثال والتدقيق، ودعم التنسيق والتدريب المشترك، والتركيز على نضج ممارسات الأمن السيبراني والامتثال وعدم الاكتفاء بمجرد وجود قسم متخصص.

الكلمات المفتاحية: التكامل الأمني، الأمن السيبراني، الأمن الرقمي، الامتثال الأمني، المنشآت الصناعية، إدارة المخاطر، رؤية المملكة العربية السعودية 2030.

المجلة الدولية لنشر البحوث والدراسات
International Journal of Research and Studies Publishing
ISSN: 2709-7064
المجلد 7 - الإصدار 81
تاريخ النشر: 20 يوليو 2026 م

The Level of Integration of Physical and Digital Security and the Relationship of Cybersecurity to Security Compliance Practices in Saudi Industrial Facilities in Light of the Kingdom of Saudi Arabia's Vision 2030

Prepared by: Sultan Saad Mohammed Al-Humaid

PhD candidate in Business Administration, Mid Ocean University, United Arab Emirates

Abstract:

The study aimed to identify the level of integration between physical and digital security, examine the relationship between the presence of a specialized cybersecurity department and the level of security compliance in Saudi industrial facilities, and interpret the findings in light of Saudi Vision 2030. The study adopted a descriptive-analytical approach and used a questionnaire to collect data from a sample of 215 participants. The data were analyzed using means and standard deviations, in addition to the Pearson Chi-Square test to examine relationships between variables and Cramer's V to assess the strength of those relationships. The findings showed that the overall level of physical and digital security integration practices was moderate, with an approximate descriptive mean of 2.83, while security compliance practices also showed a moderate level, with an approximate mean of 2.85. Moreover, 47.4% of respondents reported the presence of a specialized cybersecurity department in their facilities, compared with 52.6% who reported its absence. The Chi-Square results indicated no statistically significant relationship between the presence of a specialized cybersecurity department and the level of security compliance ($\chi 2 = 1.094, p = 0.895$), with a very weak association according to Cramer's V. Items related to digital transformation, future readiness, governance, national cybersecurity objectives, and industrial competitiveness also showed a moderate level, with an approximate descriptive mean of 2.74, highlighting the need to further develop integration practices in line with Saudi Vision 2030. The study recommended strengthening technical and organizational integration, improving security policies and compliance and auditing mechanisms, enhancing coordination and joint training, and focusing on the maturity of cybersecurity and compliance practices rather than merely establishing a specialized cybersecurity department.

Keywords: Security integration, physical security, digital security, security compliance, industrial facilities, risk management, Saudi Vision 2030.

1. المقدمة:

يشهد العالم في العقود الأخيرة تحولًا جذريًا في طبيعة التهديدات الأمنية التي تواجه المؤسسات والمنشآت الصناعية، حيث لم تعد المخاطر تقتصر على التهديدات الفيزيائية التقليدية المتمثلة في التسلل والتخريب والسرقة والاعتداء على الأصول المادية، بل امتدت لتشمل التهديدات السيبرانية والرقمية التي تستهدف الأنظمة التشغيلية وقواعد البيانات والبنية التحتية التقنية للمؤسسات. وقد أدى هذا التحول إلى ظهور بيئة أمنية معقدة تتداخل فيها المخاطر المادية مع المخاطر الرقمية بصورة متزايدة، الأمر الذي فرض على المنشآت الصناعية إعادة النظر في استراتيجياتها الأمنية التقليدية، والانتقال نحو نماذج أمنية متكاملة تجمع بين الأمن الفيزيائي والأمن الرقمي ضمن إطار موحد يضمن حماية شاملة للأصول والمعلومات والعمليات التشغيلية (Abdullah، 2025).

وتعد المنشآت الصناعية من أكثر القطاعات تعرضًا للمخاطر الأمنية المتنوعة نظرًا لما تمتلكه من أصول مادية عالية القيمة، وأنظمة تشغيل حساسة، وشبكات معلومات مترابطة تعتمد بصورة متزايدة على التقنيات الرقمية والأنظمة الذكية. ومع تسارع تطبيقات الثورة الصناعية الرابعة وانتشار تقنيات إنترنت الأشياء والذكاء الاصطناعي والحوسبة السحابية والأنظمة الصناعية المؤتمتة، أصبحت الحدود الفاصلة بين الأمن الفيزيائي والأمن السيبراني أقل وضوحًا من أي وقت مضى. فالهجمات التي تستهدف البنية الرقمية قد تؤدي إلى أضرار مادية مباشرة، كما أن الاختراقات الفيزيائية قد تكون مدخلًا للوصول إلى الأنظمة الرقمية الحساسة، مما يجعل إدارة الأمن بمعزل عن التكامل بين هذين البعدين أمرًا غير كافٍ لمواجهة التحديات الأمنية الحديثة (Zaid، 2024).

يمثل الامتثال الأمني أحد المحاور الأساسية التي تسعى المؤسسات الصناعية إلى تحقيقها في ظل التوسع المتزايد في التشريعات واللوائح والمعايير المحلية والدولية المتعلقة بالأمن وإدارة المخاطر وحماية البيانات. ويقصد بالامتثال الأمني التزام المؤسسة بالمتطلبات النظامية والتنظيمية والإجرائية التي تهدف إلى ضمان توفير مستويات مناسبة من الحماية للأصول المادية والرقمية، والحد من المخاطر المحتملة، وتحقيق معايير الجودة والاستدامة في إدارة الأمن. وتكتسب كفاءة الامتثال الأمني أهمية خاصة في المنشآت الصناعية نظرًا لما يترتب على ضعف الامتثال من خسائر مالية وتشغيلية وقانونية قد تؤثر بصورة مباشرة على استمرارية الأعمال وسمعة المؤسسة وقدرتها التنافسية (AlGhamdi، 2022).

كما أن العلاقة بين التكامل الأمني وكفاءة الامتثال الأمني أصبحت محل اهتمام متزايد من قبل الباحثين والممارسين، حيث تشير الاتجاهات الحديثة إلى أن المؤسسات التي تعتمد منهجية تكاملية في إدارة الأمن تكون أكثر قدرة على الالتزام بالمتطلبات التنظيمية وتحقيق مستويات مرتفعة من الامتثال مقارنة بالمؤسسات التي تتعامل مع الأمن الفيزيائي والأمن الرقمي بشكل منفصل. ويرجع ذلك إلى أن التكامل يسهم في توحيد الضوابط الأمنية، وتبسيط إجراءات المراجعة والتدقيق، وتحسين إدارة المخاطر، وتعزيز ثقافة الأمن المؤسسي، وهي جميعها عوامل تؤثر بصورة مباشرة في مستوى الامتثال الأمني وكفاءته (Ahmad، 2026).

تبرز أهمية دراسة مستوى التكامل بين الأمن الفيزيائي والرقمي وعلاقة الأمن السيبراني بممارسات الامتثال الأمني في المنشآت الصناعية السعودية، لما لهذا الموضوع من أبعاد استراتيجية ترتبط بتحقيق مستهدفات رؤية المملكة 2030 وتعزيز جاهزية المنشآت الصناعية لمواجهة التهديدات الأمنية المتزايدة. وتسعى هذه الدراسة إلى استكشاف طبيعة العلاقة بين التكامل الأمني بمختلف أبعاده وكفاءة الامتثال الأمني داخل المنشآت الصناعية، وتحديد مدى إسهام هذا التكامل في رفع مستويات الحماية وتقليل المخاطر وتحسين الالتزام بالمتطلبات التنظيمية والمعايير الأمنية المعتمدة. كما تسهم الدراسة في توفير إطار علمي يساعد صناع القرار ومديري الأمن وإدارات المخاطر في تطوير سياسات واستراتيجيات أمنية متكاملة تدعم الاستدامة المؤسسية وتعزز القدرة التنافسية للقطاع الصناعي السعودي في بيئة أعمال تتسم بالتغير المتسارع والتحديات المتزايدة.

1.1. مشكلة الدراسة:

في ظل التوسع المتسارع في التحول الرقمي داخل المنشآت الصناعية بالمملكة العربية السعودية، وما يصاحبه من اعتماد متزايد على الأنظمة الذكية والتقنيات الرقمية وشبكات الاتصال الصناعية، أصبحت البيئة الأمنية أكثر تعقيدًا نتيجة تداخل الأبعاد الفيزيائية والرقمية للعمليات التشغيلية. وعلى الرغم من الجهود الكبيرة التي تبذلها المنشآت الصناعية لتعزيز مستويات الحماية والالتزام بالمتطلبات الأمنية والتنظيمية، إلا أن العديد من هذه المنشآت ما تزال تتعامل مع الأمن الفيزيائي والأمن الرقمي باعتبارهما مجالين منفصلين من حيث السياسات، والإجراءات، والأنظمة الإدارية، والتقنية. ويؤدي هذا الفصل إلى ظهور فجوات أمنية تحد من القدرة على مواجهة التهديدات المعاصرة التي تتسم بالتشابك والتكامل، حيث يمكن أن يبدأ التهديد من نقطة فيزيائية وينتقل إلى الأنظمة الرقمية، أو العكس. كما أن هذا الواقع قد ينعكس سلبًا على كفاءة الامتثال الأمني من خلال صعوبة توحيد الضوابط والإجراءات الأمنية، وضعف التنسيق بين الجهات المسؤولة عن الأمن، وتكرار بعض العمليات الرقابية أو غيابها، الأمر الذي قد يؤثر في قدرة المنشآت الصناعية على تحقيق متطلبات الامتثال للمعايير والتشريعات الأمنية الحديثة. ومن هنا تتمثل المشكلة الرئيسة للدراسة في وجود حاجة متزايدة لفهم مستوى التكامل بين الأمن الفيزيائي والرقمي وعلاقة الأمن السيبراني بممارسات الامتثال الأمني في المنشآت الصناعية السعودية، ومدى إسهام هذا التكامل في تعزيز القدرة على الالتزام بالمعايير الأمنية وتحقيق مستويات أعلى من الكفاءة والجاهزية الأمنية بما يتوافق مع مستهدفات رؤية المملكة العربية السعودية 2030 (Miskini، 2026).

بناءً على مشكلة الدراسة السابقة، يمكن صياغة السؤال الرئيس للدراسة على النحو الآتي: ما مستوى التكامل بين الأمن الفيزيائي والرقمي وعلاقة الأمن السيبراني بممارسات الامتثال الأمني في المنشآت الصناعية بالمملكة العربية السعودية في ضوء مستهدفات رؤية المملكة العربية السعودية 2030؟

2.1. أسئلة الدراسة:

التساؤل الرئيس للدراسة

ما مستوى تكامل الأمن الفيزيائي والرقمي، وما طبيعة العلاقة بين وجود قسم مختص بالأمن السيبراني وممارسات التكامل والامتثال الأمني بالمنشآت الصناعية السعودية في ضوء رؤية المملكة العربية السعودية 2030؟

- **التساؤلات الفرعية للدراسة**

1. ما مستوى ممارسات تكامل الأمن الفيزيائي والرقمي بالمنشآت الصناعية السعودية؟
2. هل توجد علاقة ذات دلالة إحصائية بين الأمن السيبراني ومستوى مراقبة الأحداث الأمنية المتكاملة بالمنشآت الصناعية السعودية؟
3. هل توجد علاقة ذات دلالة إحصائية بين الأمن السيبراني ومستوى التنسيق الأمني المستمر بين فرق الأمن الفيزيائي والأمن السيبراني بالمنشآت الصناعية السعودية؟
4. هل توجد علاقة ذات دلالة إحصائية بين الأمن السيبراني ومستوى الامتثال التنظيمي الأمني بالمنشآت الصناعية السعودية؟
5. كيف يمكن تفسير نتائج مستوى التكامل والعلاقات بين متغيرات الدراسة في ضوء رؤية المملكة العربية السعودية 2030؟

3.1. أهمية الدراسة:

- **الأهمية العلمية**

تنبع الأهمية العلمية لهذه الدراسة من تناولها لموضوع حديث ومتجدد يجمع بين مجالين حيويين يشهدان اهتمامًا متزايدًا في الأدبيات

الإدارية والأمنية المعاصرة، وهما الأمن الرقمي والأمن الفيزيائي، وذلك في إطار دراسة التكامل بينهما وعلاقة الأمن السيبراني في كفاءة الامتثال الأمني داخل المنشآت الصناعية. وتكتسب الدراسة قيمتها العلمية من كونها تسهم في سد فجوة معرفية تتمثل في محدودية الدراسات العربية – وعلى وجه الخصوص الدراسات السعودية – التي تناولت العلاقة التكاملية بين هذين البعدين الأمنيين في بيئة صناعية تتسم بارتفاع مستويات المخاطر وتعقيد العمليات التشغيلية. كما تقدم الدراسة إطارًا نظريًا يربط بين مفاهيم الأمن المتكامل والامتثال الأمني وإدارة المخاطر والتحول الرقمي، الأمر الذي يسهم في إثراء الأدبيات العلمية ذات الصلة وتوسيع نطاق المعرفة الأكاديمية في هذا المجال. كذلك من المتوقع أن توفر الدراسة نتائج علمية يمكن الاستناد إليها في تطوير نماذج ونظريات مستقبلية تفسر طبيعة العلاقة بين التكامل الأمني ومستويات الامتثال داخل المؤسسات الصناعية، خاصة في ظل التطورات المتسارعة التي فرضتها الثورة الصناعية الرابعة والتوسع في استخدام الأنظمة الذكية والتقنيات الرقمية. وإضافة إلى ذلك، فإن الدراسة تقدم أساسًا علميًا يمكن أن يفيد الباحثين والدارسين في مجالات الإدارة الصناعية والأمن السيبراني وإدارة المخاطر والحوكمة المؤسسية، من خلال توفير بيانات وتحليلات تسهم في فتح آفاق جديدة للبحث العلمي حول أفضل الممارسات الأمنية التي تضمن تحقيق مستويات أعلى من الكفاءة والفاعلية التنظيمية.

- **الأهمية العملية**

تتجلى الأهمية العملية لهذه الدراسة في قدرتها على تقديم نتائج وتوصيات تطبيقية يمكن أن تسهم بصورة مباشرة في دعم جهود المنشآت الصناعية بالمملكة العربية السعودية نحو تطوير منظوماتها الأمنية وتحسين مستويات الامتثال للمتطلبات والضوابط التنظيمية المعتمدة. فمن المتوقع أن تساعد نتائج الدراسة القيادات الإدارية ومديري الأمن وإدارات المخاطر والامتثال في فهم أهمية الأمن السيبراني بوصفه مدخلًا استراتيجيًا لتعزيز الحماية الشاملة للأصول والمعلومات والعمليات التشغيلية. كما يمكن أن تسهم الدراسة في مساعدة المنشآت الصناعية على اكتشاف أوجه القصور والفجوات الأمنية الناتجة عن الفصل بين الأنظمة الأمنية المختلفة، والعمل على تطوير سياسات وإجراءات أكثر تكاملًا وفاعلية، بما يؤدي إلى رفع كفاءة إدارة المخاطر وتقليل احتمالات التعرض للحوادث الأمنية والخسائر التشغيلية والمالية. كذلك تدعم الدراسة الجهود الوطنية الرامية إلى تعزيز الأمن الصناعي والأمن السيبراني وتحقيق الاستدامة التشغيلية في القطاعات الحيوية، من خلال تقديم مؤشرات عملية حول كيفية تحسين الامتثال الأمني بما يتوافق مع المعايير الوطنية والدولية. وتزداد أهمية الدراسة العملية في ظل توجه المملكة العربية السعودية نحو بناء اقتصاد رقمي متقدم وتحقيق مستهدفات رؤية 2030، حيث يمكن الاستفادة من نتائجها في دعم صناع القرار والجهات التنظيمية عند تطوير الاستراتيجيات والسياسات الأمنية المستقبلية، بما يعزز جاهزية المنشآت الصناعية لمواجهة التحديات الأمنية المتنامية، ويرفع من مستوى تنافسيتها وقدرتها على تحقيق التنمية المستدامة في بيئة أعمال تعتمد بصورة متزايدة على التكنولوجيا والتحول الرقمي.

4.1. أهداف الدراسة:

الهدف الرئيس للدراسة: التعرف على مستوى تكامل الأمن الفيزيائي والرقمي، وتحليل العلاقة بين وجود قسم مختص بالأمن السيبراني وممارسات التكامل والامتثال الأمني بالمنشآت الصناعية السعودية، وتفسير النتائج في ضوء رؤية المملكة العربية السعودية 2030.

- **الأهداف الفرعية للدراسة:**

1. تحديد مستوى ممارسات تكامل الأمن الفيزيائي والرقمي بالمنشآت الصناعية السعودية.
2. الكشف عن العلاقة بين وجود قسم مختص بالأمن السيبراني ومستوى مراقبة الأحداث الأمنية المتكاملة بالمنشآت الصناعية السعودية.

3. الكشف عن العلاقة بين وجود قسم مختص بالأمن السيبراني ومستوى التنسيق الأمني المستمر بين فرق الأمن الفيزيائي والأمن السيبراني بالمنشآت الصناعية السعودية.
4. الكشف عن العلاقة بين وجود قسم مختص بالأمن السيبراني ومستوى الامتثال التنظيمي الأمني بالمنشآت الصناعية السعودية.
5. تفسير نتائج الدراسة في ضوء رؤية المملكة العربية السعودية 2030 ذات الصلة بالأمن السيبراني والتحول الرقمي ورفع الكفاءة المؤسسية في القطاع الصناعي.

1.5. فرضيات الدراسة:

الفرضية الرئيسة للدراسة: توجد علاقة ذات دلالة إحصائية بين وجود قسم مختص بالأمن السيبراني وممارسات التكامل والامتثال الأمني بالمنشآت الصناعية السعودية عند مستوى دلالة ($\alpha \leq 0.05$).

- **الفرضيات الفرعية للدراسة**

1. توجد علاقة ذات دلالة إحصائية بين وجود قسم مختص بالأمن السيبراني ومستوى مراقبة الأحداث الأمنية المتكاملة بالمنشآت الصناعية السعودية عند مستوى دلالة ($\alpha \leq 0.05$).
2. توجد علاقة ذات دلالة إحصائية بين وجود قسم مختص بالأمن السيبراني ومستوى التنسيق الأمني المستمر بين فرق الأمن الفيزيائي والأمن السيبراني بالمنشآت الصناعية السعودية عند مستوى دلالة ($\alpha \leq 0.05$).
3. توجد علاقة ذات دلالة إحصائية بين وجود قسم مختص بالأمن السيبراني ومستوى الامتثال التنظيمي الأمني بالمنشآت الصناعية السعودية عند مستوى دلالة ($\alpha \leq 0.05$).

2. المنطلقات النظرية للدراسة:

تشكل المنطلقات النظرية من المرتكزات الأساسية في الدراسات العلمية، إذ توفر الإطار الفكري الذي تستند إليه الدراسة في تفسير الظاهرة محل البحث وتحليل العلاقات بين متغيراتها المختلفة. كما تسهم في توجيه الباحث نحو فهم أعمق للأبعاد العلمية المرتبطة بالموضوع، من خلال الاستناد إلى النظريات والمفاهيم التي تفسر طبيعة الظاهرة المدروسة والعوامل المؤثرة فيها. وفي ظل التطورات المتسارعة التي تشهدها بيئة الأعمال الصناعية، والتزايد المستمر في التهديدات الأمنية الفيزيائية والرقمية، برزت الحاجة إلى الاعتماد على أطر نظرية متخصصة تساعد في تفسير أهمية التكامل الأمني ودوره في تعزيز كفاءة الامتثال الأمني داخل المنشآت الصناعية. وانطلاقًا من ذلك، تستند هذه الدراسة إلى مجموعة من المنطلقات والنظريات التي تفسر العلاقة بين الأمن الفيزيائي والأمن الرقمي والامتثال الأمني، وتوضح الكيفية التي يمكن من خلالها أن يسهم التكامل بين هذه الجوانب في تعزيز الحماية المؤسسية وتحقيق مستهدفات رؤية المملكة العربية السعودية 2030 المتعلقة بالأمن الصناعي والتحول الرقمي والاستدامة التنظيمية.

- **نظرية النظم**

تشكل نظرية النظم من أبرز المنطلقات النظرية التي يمكن الاستناد إليها في تفسير العلاقة بين الأمن السيبراني وكفاءة الامتثال الأمني في المنشآت الصناعية. وتنظر هذه النظرية إلى المؤسسة باعتبارها نظامًا متكاملًا يتكون من مجموعة من الأجزاء والعناصر الفرعية المترابطة التي تعمل معًا لتحقيق أهداف محددة، بحيث يؤثر أداء كل جزء في كفاءة النظام الكلي.

ووفقًا لهذا المنظور، فإن الأمن الفيزيائي والأمن الرقمي لا يمثلان نظامين منفصلين، بل عنصرين مترابطين داخل منظومة أمنية شاملة، ويتطلب تحقيق الفاعلية الأمنية وجود تنسيق وتكامل مستمر بينهما. فنجاح إجراءات الأمن الفيزيائي في حماية المواقع والمعدات والأفراد يرتبط بفاعلية الأنظمة الرقمية المسؤولة عن المراقبة والتحكم وتحليل البيانات، كما أن كفاءة الأنظمة الرقمية تعتمد بدورها

على سلامة البيئة الفيزيائية التي تعمل فيها. ومن ثم فإن أي خلل في أحد المكونات الأمنية ينعكس بصورة مباشرة على كفاءة المنظومة الأمنية بأكملها (Gamage، 2025).

- **نظرية إدارة المخاطر**

تمثل نظرية إدارة المخاطر أحد الأطر النظرية الأساسية التي تستند إليها هذه الدراسة، نظرًا لارتباطها الوثيق بعمليات تحديد المخاطر وتحليلها وتقييمها ووضع الإجراءات اللازمة للحد من آثارها المحتملة. وتفترض هذه النظرية أن المؤسسات المعاصرة تواجه بيئة عمل مليئة بالمخاطر المتنوعة والمتغيرة، الأمر الذي يتطلب تبني منهجية متكاملة لإدارة تلك المخاطر بصورة استباقية بدلًا من الاكتفاء بمعالجة آثارها بعد وقوعها. وفي المنشآت الصناعية تتنوع المخاطر بين المخاطر الفيزيائية المرتبطة بالمرافق والمعدات والعاملين، والمخاطر الرقمية المرتبطة بالأنظمة التقنية والشبكات وقواعد البيانات، وهو ما يجعل الأمن السيبراني ضرورة استراتيجية لإدارة هذه المخاطر بفاعلية (Javaid، 2023).

- **نظرية الدفاع متعدد الطبقات**

تستند هذه الدراسة كذلك إلى نظرية الدفاع متعدد الطبقات التي تُعد من أكثر النظريات استخدامًا في مجالات الأمن المؤسسي والأمن السيبراني. وترتكز هذه النظرية على فكرة أساسية مفادها أن حماية المؤسسة لا ينبغي أن تعتمد على وسيلة أمنية واحدة، وإنما على مجموعة متكاملة من الطبقات والإجراءات الأمنية التي تعمل بصورة متزامنة لتوفير حماية شاملة ضد التهديدات المختلفة. وتفترض النظرية أن فشل إحدى الطبقات الأمنية لا يعني بالضرورة نجاح التهديد، لأن الطبقات الأخرى تستمر في أداء دورها الوقائي والرقابي (Kure، 2018).

- **نظرية الامتثال التنظيمي**

تشكل نظرية الامتثال التنظيمي من المنطلقات المهمة لفهم المتغير التابع في هذه الدراسة والمتمثل في كفاءة الامتثال الأمني. وتقوم هذه النظرية على أن المؤسسات تسعى إلى الالتزام بالقوانين واللوائح والمعايير التنظيمية ليس فقط لتجنب العقوبات والمساءلة القانونية، وإنما أيضًا لتعزيز شرعيتها المؤسسية وتحسين سمعتها وزيادة ثقة أصحاب المصلحة فيها. وترى النظرية أن مستوى الامتثال يتأثر بدرجة كفاءة الأنظمة والسياسات والإجراءات المعمول بها داخل المؤسسة، ومدى قدرتها على تحقيق المتطلبات التنظيمية بصورة فعالة ومستدامة (Clemmensen، 2025).

- **نظرية التحول الرقمي المؤسسي**

تكتسب نظرية التحول الرقمي أهمية كبيرة في هذه الدراسة نظرًا لارتباطها المباشر بالتغيرات التقنية التي تشهدها المنشآت الصناعية في المملكة العربية السعودية. وتنطلق هذه النظرية من أن التطور التكنولوجي لم يعد يقتصر على إدخال أدوات وتقنيات جديدة، بل أصبح عملية تحول شاملة تؤثر في الهياكل التنظيمية والعمليات التشغيلية وأساليب الإدارة واتخاذ القرار. وقد أدى هذا التحول إلى زيادة الاعتماد على الأنظمة الرقمية الذكية في إدارة العمليات الصناعية، الأمر الذي خلق تحديات أمنية جديدة تتطلب تطوير نماذج متقدمة للحماية والرقابة (Staffenova، 2026).

3. الدراسات السابقة:

هدفت دراسة (مهران، 2024) الراهنة إلى تقديم تحليل سوسيولوجى للمخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمى ورصد آليات وجهود الدولة المصرية فى ضوء رؤية مصر 2030. لقد أظهرت النتائج أن الأمن الرقمى يعد ضرورة ملحة فرضها التطور التكنولوجى ومنظومة التحول الرقمى لضمان سلامة وأمن المعلومات وتكنولوجيا الاتصالات. بيَّنت النتائج أن معظم

دول العالم تعرَّضت للعديد من الجرائم والهجمات السيبرانية التي استهدفت القطاعات الحيوية فى المجتمع، ومن ثم قامت بإصدار القوانين المختلفة من أجل التغلب على التهديدات والأخطار الناجمة عنها. أوضحت النتائج أن مصر من أوائل الدول التي قامت بسن التشريعات والقوانين وإنشاء المراكز والمجالس المتخصصة، ووضع الكثير من الاستراتيجيات التي تتضمن العديد من البرامج الاستراتيجية المختلفة، وعقد المؤتمرات من أجل حماية الدولة من مخاطر الجرائم والهجمات السيبرانية، ولتحقيق بيئة رقمية آمنة وموثوقة للمجتمع المصري بمختلف أطيافه.

تتناول دراسة (Agrawal، 2022) الجانب الأمني لأنظمة الفضاء الإلكتروني الفيزيائي الصناعية، وتقدم مسحاً شاملاً على مدى عقد من الزمن، يشمل مختلف الثغرات الأمنية والهجمات ومكونات أنظمة الفضاء الإلكتروني الفيزيائي، بالإضافة إلى جوانب أخرى متعددة. كما تُقدم الدراسة تحليلاً مقارناً سنوياً للأعمال المنشورة، من حيث الهدف والمنهجية المتبعة وبيئة الاختبار المستخدمة والاستنتاجات المستخلصة. علاوة على ذلك، تُفصّل الدراسة مختلف القضايا الأمنية والتحديات البحثية التي تواجه أنظمة الفضاء الإلكتروني الفيزيائي الصناعية. وتسعى هذه الدراسة إلى تقديم دراسة أدبية موجزة ودقيقة تركز على أحدث ما توصل إليه أمن أنظمة الفضاء الإلكتروني الفيزيائي الصناعية. كما تشجع هذه الدراسة الباحثين الشباب على استكشاف الإمكانيات الواسعة المتاحة في هذا المجال الناشئ.

تهدف دراسة (خشبة، 2021) إلى تحليل دور الأمن السيبراني كأحد التوجهات الاستراتيجية الحديثة في دعم التنمية المستدامة والاقتصاد القائم على المعرفة والتحول الرقمي، مع التركيز على إسهامه في حماية الأصول الرقمية وتعزيز الأمن القومي في ظل تصاعد التهديدات الإلكترونية عالميًا. وتنطلق الدراسة من تنامي الاهتمام الدولي والإقليمي بالأمن السيبراني باعتباره أحد التقنيات الحاكمة في مستقبل التنمية إلى جانب الذكاء الاصطناعي وسلاسل الكتل والتكنولوجيا الحيوية، كما تستعرض تطور هذا المجال في مصر من خلال إنشاء مؤسسات واستراتيجيات وطنية متخصصة لمواجهة المخاطر السيبرانية وتعزيز الجاهزية الرقمية. وتناقش الدراسة العلاقة بين الأمن السيبراني والتحول الرقمي والاقتصاد المعرفي، إضافة إلى دوره في دعم القطاعات الحكومية والتنموية، ومواجهة التحديات المرتبطة بالحروب السيبرانية والتهديدات الرقمية التي تمثل أحد أبرز مخاطر الأمن القومي في العصر الحديث.

تستكشف دراسة (Alhussain، 2026). الأثر البيئي للحوسبة السحابية في المملكة العربية السعودية، مع التركيز على مدى توافقها مع رؤية 2030 والمبادرة الخضراء السعودية. وتدرس كيف تُحفز تقنيات الحوسبة السحابية الابتكار والنمو الاقتصادي، في حين تُساهم في انبعاثات الكربون والنفايات الإلكترونية. وتستعرض الدراسة الأدبيات التي تُبين حلولًا مُحتملة، مثل تبني الطاقة المتجددة، واستخدام المحاكاة الافتراضية، وتقنيات احتجاز الكربون، والممارسات الصديقة للبيئة في مراكز البيانات. ورغم هذه الجهود، لا تزال هناك فجوات في البحث وتطبيق السياسات تُشكل عوائق أمام تحقيق صافي انبعاثات صفري. وتؤكد الدراسة على الحاجة إلى استراتيجيات شاملة ومزيد من البحث لتحقيق التوازن بين الرقمنة والاستدامة البيئية، لضمان توافق الحوسبة السحابية مع أهداف المملكة طويلة الأجل.

التعليق على الدراسات السابقة:

- **أوجه التشابه في الدراسات السابقة**

تتفق الدراسات السابقة في تركيزها على أهمية الأمن السيبراني والتحول الرقمي بوصفهما من الركائز الأساسية في دعم التنمية المستدامة وحماية الأصول الرقمية وتعزيز الأمن القومي في ظل التوسع المتزايد في استخدام التقنيات الحديثة. كما تشترك هذه الدراسات في إبراز تصاعد التهديدات السيبرانية والهجمات الإلكترونية التي تستهدف القطاعات الحيوية، وما يترتب عليها من تحديات

أمنية وتنظيمية تتطلب تطوير أطر استراتيجية وتشريعية وتقنية لمواجهتها. كذلك، تتقاطع الدراسات في التأكيد على أهمية التكامل بين التقنيات الحديثة والأنظمة المؤسسية، سواء في سياق الأنظمة الصناعية السيبرانية الفيزيائية أو في إطار التحول الرقمي، بالإضافة إلى إبراز دور الدولة والمؤسسات في بناء استراتيجيات وطنية لتعزيز الأمن الرقمي ومواكبة التطورات العالمية.

- **أوجه الاختلاف في الدراسات السابقة**

تختلف الدراسات السابقة من حيث الزاوية البحثية والتركيز الموضوعي؛ إذ ركزت بعض الدراسات على البعد السوسيولوجي للمخاطر السيبرانية وانعكاساتها على المجتمع والسياسات العامة، بينما تناولت دراسات أخرى الجوانب التقنية والهندسية المرتبطة بأنظمة الفضاء الإلكتروني الفيزيائي والتحديات الأمنية داخل البيئات الصناعية. في المقابل، اتجهت دراسات أخرى إلى تحليل دور الأمن السيبراني في دعم التنمية المستدامة والاقتصاد القائم على المعرفة والتحول الرقمي، مع التركيز على الأبعاد الاستراتيجية والأمن القومي. كما تميزت بعض الدراسات بالتركيز على قطاعات محددة مثل الحوسبة السحابية والأثر البيئي والتقني لها، في حين لم تتناول بشكل مباشر التكامل بين الأمن الفيزيائي والأمن الرقمي داخل المنشآت الصناعية، وأثر الأمن السيبراني على كفاءة الامتثال الأمني بشكل تفصيلي.

- **الفجوات البحثية التي يميزها البحث الحالي**

يتضح من تحليل الدراسات السابقة وجود فجوة بحثية تتمثل في محدودية الدراسات التي تناولت التكامل بين الأمن الفيزيائي والأمن الرقمي، خاصة في السياق السعودي المرتبط برؤية المملكة 2030. كما أن معظم الدراسات ركزت على الأمن السيبراني بمعزل عن الأمن الفيزيائي، أو تناولت التهديدات السيبرانية من منظور تقني أو تنظيمي دون الربط الشامل بين الجانبين في إطار تكاملي. بالإضافة إلى ذلك، هناك نقص في الدراسات التطبيقية التي تقيس العلاقة بين الأمن السيبراني بممارسات الامتثال الأمني ميدانيًا باستخدام بيانات كمية من داخل المنشآت الصناعية، وتحدد علاقته الفعلية على الامتثال الأمني وإدارة المخاطر. ومن ثم، تسعى الدراسة الحالية إلى سد هذه الفجوة من خلال تقديم نموذج تحليلي توضح التكامل بين الأمن الفيزيائي والرقمي، بما يدعم متطلبات التحول الرقمي ويعزز تحقيق مستهدفات رؤية المملكة العربية السعودية 2030.

4. المنهجية وطرق البحث:

1.4. منهج الدراسة:

اعتمدت الدراسة على المنهج الوصفي التحليلي بوصفه المنهج الأكثر ملاءمة لطبيعة الدراسة وأهدافها، حيث يركز هذا المنهج على وصف الظاهرة المدروسة وصفًا دقيقًا من خلال جمع البيانات المتعلقة بها وتحليلها وتفسيرها بصورة علمية. ويُعد المنهج الوصفي التحليلي من أكثر المناهج استخدامًا في الدراسات الإدارية والتنظيمية؛ نظرًا لقدرته على دراسة العلاقات بين المتغيرات المختلفة والكشف عن اتجاهاتها المتبادلة.

وقد تم توظيف هذا المنهج لدراسة واقع التكامل بين الأمن الفيزيائي والأمن الرقمي داخل المنشآت الصناعية السعودية، والتعرف على مستوى كفاءة الامتثال الأمني فيها، بالإضافة إلى تحليل طبيعة العلاقة بين المتغير المستقل المتمثل في الأمن السيبراني والمتغير التابع المتمثل في كفاءة الامتثال الأمني. كما يتيح هذا المنهج إمكانية تحليل آراء أفراد العينة واستخلاص المؤشرات التي تساعد على فهم علاقة وجود قسم مختص للأمن السيبراني في تعزيز الالتزام بالمعايير والضوابط الأمنية المعتمدة. ويساعد كذلك في تقديم صورة واقعية وشاملة عن الممارسات الأمنية السائدة داخل المنشآت الصناعية ومدى توافقها مع التوجهات الحديثة في الأمن المؤسسي وإدارة المخاطر.

2.4. مجتمع الدراسة

يتكون مجتمع الدراسة من العاملين والقيادات الإدارية والمتخصصين في مجالات الأمن الفيزيائي والأمن السيبراني وإدارة المخاطر والامتثال الأمني في المنشآت الصناعية بالمملكة العربية السعودية. ويشمل ذلك المديرين والمشرفين والموظفين ذوي العلاقة المباشرة بالأنشطة الأمنية والتنظيمية داخل المنشآت الصناعية، باعتبارهم الأكثر معرفة بالممارسات الأمنية المطبقة ومستوى التكامل بين الأنظمة الأمنية المختلفة، فضلًا عن قدرتهم على تقييم مستوى الامتثال الأمني داخل مؤسساتهم.

وقد تم اختيار هذا المجتمع نظرًا لارتباطه المباشر بمتغيرات الدراسة، حيث يمثل المصدر الأساسي للمعلومات المتعلقة بواقع التكامل الأمني ومدى انعكاسه على كفاءة الامتثال الأمني في البيئة الصناعية السعودية. كما أن طبيعة مهام أفراد هذا المجتمع تمنحهم القدرة على تقديم تقييمات واقعية ودقيقة تسهم في تحقيق أهداف الدراسة والوصول إلى نتائج ذات دلالة علمية وعملية.

3.4. عينة الدراسة

نظرًا لصعوبة الوصول إلى جميع أفراد مجتمع الدراسة واتساع نطاقه الجغرافي وتعدد المنشآت الصناعية بالمملكة العربية السعودية، فقد تم الاعتماد على العينة العشوائية البسيطة باعتبارها من أكثر أساليب المعاينة ملاءمة للدراسات الوصفية التحليلية، حيث تتيح الفرصة لجميع أفراد المجتمع للدخول في العينة بدرجات متساوية، مما يعزز من موضوعية النتائج وإمكانية تعميمها على المجتمع الأصلي.

وقد بلغ حجم عينة الدراسة (215) مفردة من العاملين والمتخصصين في المجالات الأمنية والإدارية داخل المنشآت الصناعية السعودية. ويُعد هذا الحجم مناسبًا لإجراء التحليلات الإحصائية المطلوبة واختبار فرضيات الدراسة بدرجة مقبولة من الدقة والثقة الإحصائية. كما يسهم هذا العدد في توفير تمثيل مناسب لآراء أفراد المجتمع المستهدف، الأمر الذي يعزز من موثوقية النتائج المستخلصة ويزيد من قدرتها على تفسير العلاقة بين الأمن السيبراني وكفاءة الامتثال الأمني في المنشآت الصناعية بالمملكة العربية السعودية.

4.4. حدود الدراسة:

- **الحدود البشرية:** تقتصر الدراسة من الناحية البشرية على العاملين والقيادات الإدارية والمتخصصين في مجالات الأمن الفيزيائي والأمن السيبراني وإدارة المخاطر والامتثال الأمني داخل المنشآت الصناعية بالمملكة العربية السعودية.
- **الحدود الزمانية:** تتمثل الحدود الزمانية للدراسة في الفترة التي تم خلالها جمع البيانات الميدانية وتحليلها وإجراء الدراسة، وهي عام 2026م .ويأتي اختيار هذه الفترة نظرًا لما تشهده المملكة العربية السعودية خلالها من تسارع في تنفيذ برامج التحول الرقمي وتطوير البنية التحتية للأمن السيبراني والصناعي ضمن إطار رؤية المملكة العربية السعودية 2030. كما تعكس هذه الفترة واقع الممارسات الأمنية الحديثة والتحديات المعاصرة المرتبطة بتكامل الأمن الفيزيائي والرقمي داخل المنشآت الصناعية، الأمر الذي يجعل النتائج المستخلصة أكثر ارتباطًا بالبيئة التنظيمية والتقنية الحالية التي تعمل في ظلها المؤسسات الصناعية السعودية.
- **الحدود المكانية:** تقتصر الدراسة من الناحية المكانية على المنشآت الصناعية العاملة في المملكة العربية السعودية بمختلف قطاعاتها الصناعية، سواء كانت منشآت صناعية كبيرة أو متوسطة أو ذات طبيعة تشغيلية تعتمد على الأنظمة التقنية والرقمية في إدارة عملياتها. ويأتي اختيار المملكة العربية السعودية ميدانًا للدراسة نظرًا لما يشهده القطاع الصناعي فيها من نمو متسارع وتوسع في تطبيق تقنيات الثورة الصناعية الرابعة والتحول الرقمي، إلى جانب الاهتمام الكبير الذي توليه الجهات الحكومية لتعزيز الأمن

الصناعي والأمن السيبراني ورفع مستويات الامتثال للمعايير والضوابط الأمنية. كما يرتبط اختيار هذا النطاق المكاني ارتباطًا مباشرًا بموضوع الدراسة الذي يسعى إلى استكشاف دور التكامل الأمني في دعم مستهدفات رؤية المملكة العربية السعودية 2030 وتحقيق متطلبات التنمية الصناعية المستدامة في بيئة عمل تتسم بالتطور التقني والتنافسية العالية.

5.4. أداة الدراسة:

لتحقيق أهداف الدراسة، قام الباحث بتطوير "استبانة" كأداة رئيسة لجمع البيانات الأولية من أفراد العينة. وقد تم بناء الأداة استناداً إلى الأدبيات السابقة والدراسات ذات الصلة بمجالات الأمن المتكامل والامتثال الأمني. تتكون الأداة في صورتها النهائية من (31) عبارة. وللتحقق من موثوقية أداة الدراسة تم حساب معامل الموثوقية لبنود الاستبيان. وأظهرت النتائج أن معامل ألفا كرونباخ للبنود الرئيسية بلغ 0.818، وهو رقم مرتفع يتجاوز الحد المقبول إحصائيًا (0.70). وهذا يدل على أن الأداة تتمتع بدرجة عالية من الاتساق والموثوقية، ويمكن الاعتماد عليها في تعميم النتائج.

جدول (1) معامل الثبات الفا كرونباخ لأداة الدراسة

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.818	.809	31

6.4. أساليب التحليل الإحصائي:

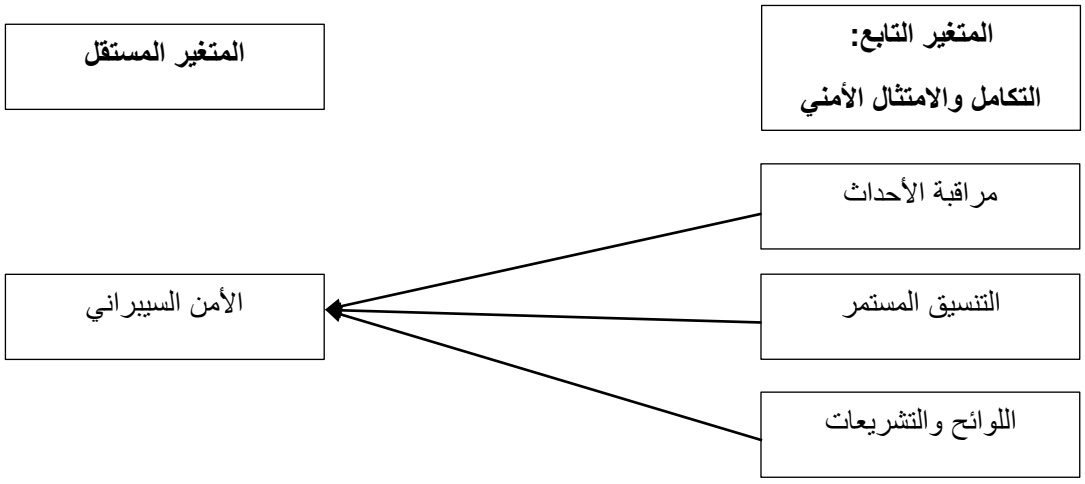
استُخدم برنامج SPSS لمعالجة البيانات المُستقاة من الاستبيان، وذلك لتحقيق أهداف الدراسة وتقييم فرضياتها. تمكّن المشاركون من تحديد مدى موافقتهم على عبارات الدراسة باستخدام مقياس ليكرت خماسي النقاط. وتم تطبيق الأوزان التالية على الإجابات: (5 نقاط للموافقة التامة، 4 نقاط للموافقة، 3 نقاط للحياد، نقطتان للرفض، ونقطة واحدة للرفض التام). استُخدمت الأساليب الإحصائية التالية:

- معامل ألفا لكرونباخ لتقييم الاتساق الداخلي وموثوقية أداة البحث، والتأكد من أن العبارات تقيس المتغيرات المطلوبة بدقة وثبات.
- التكرارات والنسب المئوية والمتوسطات الحسابية لتقييم كل عبارة من عبارات الدراسة وفقًا لأهميتها، وتحديد درجة الموافقة بين أفراد العينة.
- الانحرافات المعيارية لقياس مدى تباين إجابات أفراد العينة عن المتوسط الحسابي، مما يدل على مدى تجانس آرائهم.
- الالتواء والتفرطح للتأكد من أن توزيع البيانات طبيعي ومناسب للاختبارات الإحصائية المعلمية.
- اختبار مربع كاي يُستخدم في الاختبارات المتقاطعة لدراسة العلاقة بين العوامل النوعية، مثل وظيفة الأمن السيبراني وعلاقتها بالتنسيق المستمر أو القوانين واللوائح داخل الشركات.
- عامل بايز: يهدف إلى تعزيز موثوقية النتائج العلمية للدراسة من خلال مقارنة الفرضية الصفرية بالفرضية البديلة، وتقديم المزيد من الأدلة على نتائج النماذج الإحصائية.

7.4. متغيرات الدراسة:

تتكون الدراسة من متغير مستقل يتمثل في الأمن السيبراني، والذي تم قياسه إجرائيًا من خلال وجود قسم مختص بالأمن السيبراني داخل المنشأة من عدمه، ومتغير تابع مفاهيمي يتمثل في مستوى ممارسات التكامل والامتثال الأمني، والذي تمثله إجرائيًا ثلاثة مؤشرات هي مراقبة الأحداث الأمنية المتكاملة، والتنسيق الأمني المستمر، والامتثال التنظيمي الأمني. وقد عولج كل مؤشر من المؤشرات الثلاثة بوصفه متغيرًا تابعًا رتبيًا مستقلًا عند اختبار الأثر إحصائيًا:

شكل (1) متغيرات الدراسة



5. نتائج الدراسة وتحليلها:

يعرض هذا الفصل نتائج الدراسة الميدانية المتعلقة بمستوى تكامل الأمن الفيزيائي والرقمي، وعلاقة وجود قسم للأمن السيبراني في ممارسات التكامل والامتثال الأمني بالمنشآت الصناعية السعودية. ويبدأ الفصل بعرض الخصائص العامة لعينة الدراسة والخصائص التنظيمية للمنشآت، ثم يقدم الإحصاءات الوصفية لبنود الاستبانة والمجالات التي تناولتها، يلي ذلك اختبار العلاقات الإحصائية، ثم اختبار علاقة الأمن وجود قسم للأمن السيبراني باستخدام اختبارات كاي سكوير تربيع.

وقد تناولت الاستبانة عددًا من المجالات الوصفية المرتبطة بموضوع الدراسة، تمثلت في: التكامل التقني بين الأمن الفيزيائي والرقمي، والتنسيق التنظيمي والتشغيلي، والتدريب والوعي والجاهزية الأمنية، والامتثال الأمني، والنتائج التشغيلية للتكامل، والإسهامات الاستراتيجية المرتبطة بالتكامل الأمني.

أما في نموذج التحليل الاستدلالي، فيتمثل المتغير المستقل في الأمن السيبراني، والذي قيس إجرائيًا من خلال وجود قسم مختص بالأمن السيبراني داخل المنشأة من عدمه. وتمثلت المتغيرات التابعة الرتبية في ثلاثة مؤشرات هي: مراقبة الأحداث الأمنية المتكاملة، والتنسيق الأمني المستمر، والامتثال التنظيمي الأمني. وقد تم تحليل كل مؤشر منها بوصفه متغيرًا تابعًا رتبيًا مستقلًا.

كما تم توظيف رؤية المملكة العربية السعودية 2030 إطارًا نظريًا واستراتيجيًا لتفسير نتائج الدراسة ومناقشة دلالاتها، دون معاملتها بوصفها متغيرًا إحصائيًا ضمن نموذج التحليل. بلغ حجم عينة الدراسة 215 مشاركًا، وكانت جميع الاستجابات المدرجة في التحليل صالحة وفق ملخص معالجة الحالات.

1.5. الإحصاءات الوصفية لاستجابات أفراد العينة على بنود الاستبانة:

جدول (2) الإحصاءات الوصفية لاستجابة أفراد عينة الدراسة على بنود الاستبيان

Statistics						
Kurtosis	Skewness	Std. Deviation	Std. Error of Mean	Mean	N Valid	
-2.008	0.103	0.501	0.034	1.47	215	هل يوجد في منشأتكم قسم مختص بالأمن السيبراني؟
-2.018	0.028	0.501	0.034	1.49	215	هل تطبق المنشأة أنظمة أمن فيزيائي ورقمي متكاملة؟
-1.374	0.126	1.465	0.100	2.80	215	توجد أنظمة مترابطة بين الأمن الفيزيائي والأمن الرقمي في المنشأة.
-1.285	0.260	1.452	0.099	2.74	215	يتم ربط أنظمة المراقبة والكاميرات بالأنظمة الرقمية الأمنية.
-1.405	0.122	1.483	0.101	2.87	215	تستخدم المنشأة منصة موحدة لمراقبة الأحداث الأمنية الفيزيائية والرقمية.
-1.350	0.246	1.512	0.103	2.74	215	تتكامل أنظمة التحكم في الدخول مع أنظمة إدارة الهوية الرقمية.
-1.462	0.167	1.538	0.105	2.86	215	يتم تبادل البيانات الأمنية بين الأنظمة الفيزيائية والرقمية بشكل آلي.
-1.378	-0.083	1.474	0.101	3.03	215	يوجد تنسيق مستمر بين فرق الأمن الفيزيائي والأمن السيبراني.
-1.320	0.190	1.447	0.099	2.77	215	تعقد اجتماعات دورية لمناقشة المخاطر الأمنية المشتركة.
-1.378	0.053	1.461	0.100	2.86	215	توجد سياسات موحدة تشمل الأمن الفيزيائي والرقمي.
-1.334	0.069	1.450	0.099	2.90	215	تشارك الإدارات الأمنية في وضع الخطط والاستراتيجيات الأمنية.
-1.347	0.112	1.458	0.099	2.88	215	يتم التنسيق المشترك عند التعامل مع الحوادث الأمنية.

تقدم المنشأة برامج تدريبية تجمع بين مفاهيم الأمن الفيزيائي والرقمي.	215	2.76	0.102	1.491	0.174	-1.389
يمتلك الموظفون وعياً كافياً بالمخاطر الأمنية المترابطة.	215	2.93	0.098	1.440	-0.019	-1.318
يتم تنفيذ تمارين ومحاكاة للحوادث الأمنية المشتركة.	215	2.79	0.096	1.414	0.175	-1.268
تقوم المنشأة بتحديث برامج التوعية الأمنية بشكل دوري.	215	2.69	0.094	1.377	0.350	-1.116
يساهم التدريب الأمني في تعزيز التعاون بين الفرق الأمنية.	215	2.84	0.102	1.493	0.137	-1.441
تلتزم المنشأة باللوائح والتشريعات الأمنية المعمول بها.	215	2.90	0.102	1.490	0.126	-1.434
تطبق المنشأة متطلبات الأمن السيبراني المعتمدة من الجهات التنظيمية.	215	2.85	0.102	1.491	0.104	-1.420
يتم تحديث السياسات الأمنية بما يتوافق مع المتطلبات النظامية.	215	2.87	0.100	1.473	0.085	-1.407
تخضع المنشأة لمراجعات وتدقيقات أمنية دورية.	215	2.78	0.100	1.470	0.224	-1.349
توجد آليات واضحة لمتابعة الامتثال الأمني.	215	2.86	0.098	1.435	0.045	-1.330
يساعد التكامل بين الأمن الفيزيائي والرقمي على سرعة الاستجابة للحوادث.	215	2.79	0.099	1.456	0.113	-1.377
يساعد التكامل بين الأمن الفيزيائي والرقمي على سرعة الاستجابة للحوادث.	215	2.75	0.104	1.520	0.207	-1.448
يساهم التكامل الأمني في تقليل الحوادث الأمنية.	215	2.83	0.094	1.374	0.174	-1.200
يساعد التكامل الأمني في تعزيز استمرارية الأعمال.	215	2.81	0.100	1.467	0.102	-1.346

يسهم التكامل بين الأمن الفيزيائي والرقمي في دعم التحول الرقمي.	215	2.67	0.098	1.440	0.281	-1.276
يساعد التكامل الأمني على تعزيز جاهزية المنشآت الصناعية للمستقبل.	215	2.84	0.102	1.490	0.180	-1.399
يساهم التكامل الأمني في رفع مستوى الحوكمة والامتثال.	215	2.73	0.100	1.464	0.261	-1.329
يدعم التكامل الأمني تحقيق مستهدفات الأمن السيبراني الوطنية.	215	2.79	0.098	1.434	0.199	-1.308
يساهم التكامل الأمني في تعزيز تنافسية المنشآت الصناعية السعودية.	215	2.69	0.101	1.488	0.290	-1.320

تظهر النتائج الوصفية أن متوسطات بنود مقياس ليكرت الخماسي تراوحت بين (2.67) و(3.03)، وهي جميعها ضمن مستوى الاستجابة المتوسط وفق معيار التفسير المعتمد. وسجلت عبارة «يوجد تنسيق مستمر بين فرق الأمن الفيزيائي والأمن السيبراني» أعلى متوسط حسابي بلغ (3.03)، تلتها عبارة «يمتلك الموظفون وعياً كافياً بالمخاطر الأمنية المترابطة» بمتوسط (2.93)، ثم عبارة «تشارك الإدارات الأمنية في وضع الخطط والاستراتيجيات الأمنية» وعبارة «تلتزم المنشأة باللوائح والتشريعات الأمنية المعمول بها» بمتوسط بلغ (2.90) لكل منهما. وتشير هذه النتائج إلى أن التنسيق والوعي والمشاركة التنظيمية والامتثال كانت من أكثر الممارسات حضورًا نسبيًا لدى أفراد العينة، مع بقائها ضمن المستوى المتوسط.

وفي المقابل، سجلت عبارة «يسهم التكامل بين الأمن الفيزيائي والرقمي في دعم التحول الرقمي» أدنى متوسط بين بنود مقياس ليكرت وبلغ (2.67)، تلتها عبارة «يساهم التكامل الأمني في تعزيز تنافسية المنشآت الصناعية السعودية» بمتوسط (2.69)، وهو ما يشير إلى أن التقديرات المتعلقة بالمخرجات الاستراتيجية بعيدة المدى للتكامل كانت أقل نسبيًا من بعض الممارسات التنظيمية والتشغيلية، مع بقائها كذلك ضمن المستوى المتوسط.

وبشكل عام، تعكس النتائج الوصفية مستوى متوسطًا لممارسات تكامل الأمن الفيزيائي والرقمي في المنشآت محل الدراسة، سواء في الجوانب التقنية أو التنظيمية أو التدريبية والتوعوية، كما أظهرت بنود الامتثال الأمني مستويات متوسطة. ولا تمثل هذه النتائج الوصفية في حد ذاتها دليلًا على وجود أثر إحصائي للتنظيم المؤسسي للأمن السيبراني، إذ سيتم اختبار ذلك بصورة مستقلة باستخدام الاختبارات الاستدلالية والانحدار اللوجستي الرتبي في الأجزاء اللاحقة من الفصل.

2.5. اختبار العلاقة بين الأمن السيبراني ومؤشرات ممارسات التكامل والامتثال الأمني:

تم استخدم اختبار كاي تربيع (Pearson Chi-Square) للكشف عن وجود علاقة إحصائية بين الأمن السيبراني، المقاس إجرائيًا بوجود قسم مختص بالأمن السيبراني داخل المنشأة من عدمه، وكل من مراقبة الأحداث الأمنية المتكاملة، والتنسيق الأمني المستمر، والامتثال التنظيمي الأمني. ويعد هذا التحليل اختبارًا أوليًا لطبيعة العلاقة بين المتغيرات، في حين يستخدم الانحدار اللوجستي الرتبي (Ordinal Logistic Regression) لاحقًا لاختبار الأثر الإحصائي للتنظيم المؤسسي للأمن السيبراني في مستويات المؤشرات التابعة. كما استخدم معامل Cramer's V لتقدير قوة العلاقة.

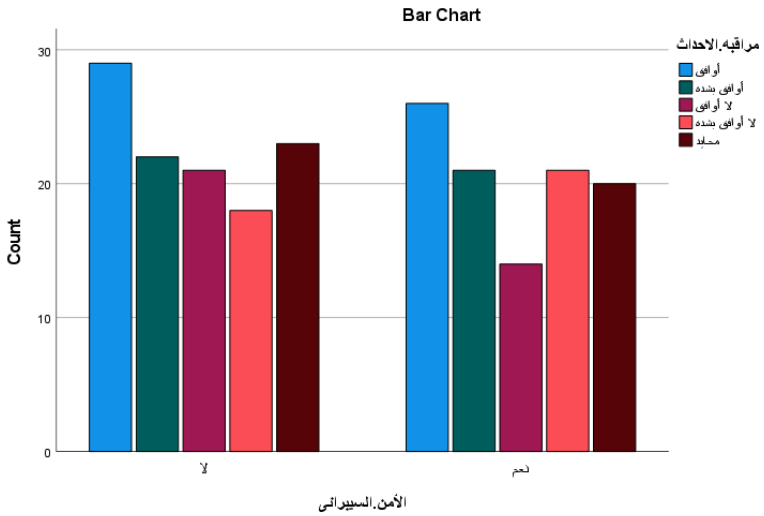
ـ العلاقة بين الأمن السيبراني ومراقبة الأحداث الأمنية المتكاملة في المنشأت الصناعية بالمملكة العربية السعودية

جدول (3) نتائج اختبار كاي تربيع للعلاقة بين الأمن السيبراني ومستوى مراقبة الأحداث الأمنية المتكاملة بالمنشآت الصناعية السعودية

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1.468[a]	4	.832
Likelihood Ratio	1.474	4	.831
Linear-by-Linear Association	.014	1	.906
N of Valid Cases	215		
a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 16.60.			

يوضح جدول (3) نتائج اختبار كاي تربيع للكشف عن العلاقة بين الأمن السيبراني، المقاس بوجود قسم مختص بالأمن السيبراني من عدمه، ومستوى مراقبة الأحداث الأمنية المتكاملة، الذي تمثله العبارة «تستخدم المنشأة منصة موحدة لمراقبة الأحداث الأمنية الفيزيائية والرقمية». وقد بلغت قيمة كاي تربيع لبيرسون ($\chi^2 = 1.468$) بدرجات حرية ($df = 4$)، وبلغ مستوى الدلالة الإحصائية ($p = 0.832$)، وهو أكبر من مستوى الدلالة المعتمد ($\alpha = 0.05$). وبناءً على ذلك، لا توجد أدلة إحصائية كافية على وجود علاقة ذات دلالة إحصائية بين وجود قسم مختص بالأمن السيبراني ومستوى مراقبة الأحداث الأمنية المتكاملة لدى المنشآت محل الدراسة. ويعني ذلك أن توزيع مستويات الاستجابة المتعلقة بمراقبة الأحداث الأمنية المتكاملة لم يختلف بصورة دالة إحصائيًا باختلاف وجود قسم مختص بالأمن السيبراني من عدمه. كما أظهرت نتائج الاختبار استيفاء شرط التكرارات المتوقعة، إذ لم توجد أي خلية ذات تكرار متوقع أقل من (5)، وبلغ الحد الأدنى للتكرار المتوقع (16.60)، مما يدعم ملاءمة استخدام اختبار كاي تربيع لهذه البيانات.

شكل (2) توزيع استجابات أفراد العينة حول مستوى مراقبة الأحداث الأمنية المتكاملة وفق وجود قسم مختص بالأمن السيبراني بالمنشآت الصناعية السعودية



- العلاقة بين الأمن السيبراني ومستوى التنسيق الأمني المستمر بين فرق الأمن الفيزيائي والأمن السيبراني.

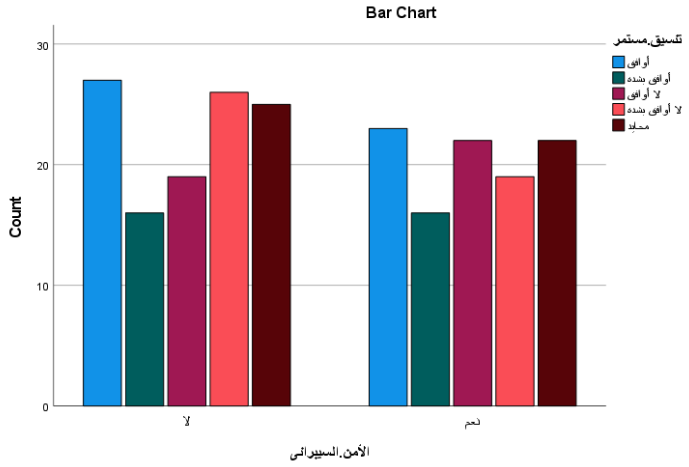
جدول (4) نتائج اختبار كاي تربيع للعلاقة بين الأمن السيبراني ومستوى التنسيق الأمني المستمر بالمنشآت الصناعية السعودية.

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1.260[a]	4	.868
Likelihood Ratio	1.262	4	.868
Linear-by-Linear Association	.046	1	.830
N of Valid Cases	215		
a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 15.18.			

يوضح جدول (4) نتائج اختبار كاي تربيع للكشف عن العلاقة بين وجود قسم مختص بالأمن السيبراني ومستوى التنسيق الأمني المستمر بين فرق الأمن الفيزيائي والأمن السيبراني. وقد بلغت قيمة كاي تربيع لبيرسون ($\chi^2 = 1.260$) بدرجات حرية ($df = 4$)، وبلغ مستوى الدلالة الإحصائية ($p = 0.868$)، وهي قيمة أكبر من مستوى الدلالة المعتمد ($\alpha = 0.05$). وبناءً على ذلك، لا توجد أدلة إحصائية كافية على وجود علاقة ذات دلالة إحصائية بين وجود قسم مختص بالأمن السيبراني ومستوى التنسيق الأمني المستمر في المنشآت الصناعية محل الدراسة. ويشير ذلك إلى أن مستويات التنسيق المبلغ عنها لم تختلف بصورة دالة إحصائيًا بين المنشآت التي يوجد فيها قسم مختص بالأمن السيبراني والمنشآت التي لا يوجد فيها قسم مختص. كما لم توجد أي خلايا ذات تكرارات متوقعة أقل من (5)، وبلغ الحد الأدنى للتكرار المتوقع (15.18)، مما يؤكد تحقق أحد الشروط الأساسية لاستخدام اختبار كاي تربيع.

ويمكن تفسير عدم دلالة العلاقة بأن وجود قسم مختص بالأمن السيبراني يمثل مؤشرًا على الوجود التنظيمي الرسمي للأمن السيبراني، لكنه لا يعكس بالضرورة مستوى نضج آليات التنسيق والتعاون الفعلي بين فرق الأمن السيبراني والأمن الفيزيائي. فقد تمارس بعض المنشآت وظائف الأمن السيبراني من خلال فرق مشتركة أو إدارات أخرى أو جهات خارجية دون وجود قسم مستقل، كما أن مجرد وجود قسم متخصص لا يضمن بالضرورة تحقق التنسيق المستمر بين الفرق الأمنية.

شكل (3) توزيع استجابات أفراد العينة حول مستوى التنسيق الأمني المستمر وفق وجود قسم مختص بالأمن السيبراني بالمنشآت الصناعية السعودية



ـ العلاقة بين الأمن السيبراني والامتثال التنظيمي للوائح والتشريعات بالمنشات الصناعية بالمملكة العربية السعودية

جدول (5) نتائج اختبار كاي تربيع للعلاقة بين الأمن السيبراني ومستوى الامتثال التنظيمي الأمني للوائح والتشريعات بالمنشآت الصناعية السعودية.

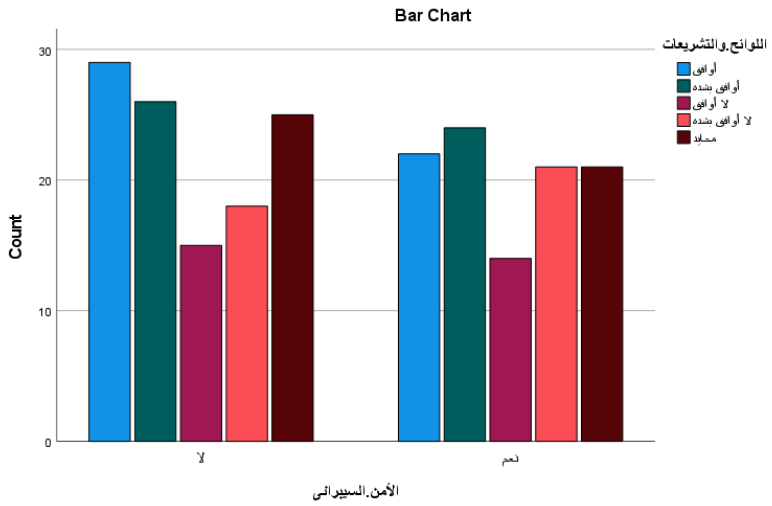
Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1.094[a]	4	.895
Likelihood Ratio	1.095	4	.895
Linear-by-Linear Association	.207	1	.649
N of Valid Cases	215		
a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 13.76.			

يوضح جدول (5) نتائج اختبار كاي تربيع للكشف عن العلاقة بين الأمن السيبراني ومستوى الامتثال التنظيمي الأمني، الذي تمثله العبارة «تلتزم المنشأة باللوائح والتشريعات الأمنية المعمول بها». وقد بلغت قيمة كاي تربيع لبيرسون ($\chi^2 = 1.094$) بدرجات حرية ($df = 4$)، وبلغ مستوى الدلالة الإحصائية ($p = 0.895$)، وهي قيمة أكبر من مستوى الدلالة المعتمد ($\alpha = 0.05$).

وبناءً على ذلك، لا توجد أدلة إحصائية كافية على وجود علاقة ذات دلالة إحصائية بين وجود قسم مختص بالأمن السيبراني ومستوى الامتثال التنظيمي الأمني في المنشآت الصناعية محل الدراسة. وتشير النتيجة إلى أن مستويات الالتزام باللوائح والتشريعات الأمنية لم تختلف بصورة دالة إحصائيًا باختلاف وجود قسم مختص بالأمن السيبراني من عدمه.

كما لم تسجل أي خلية تكرارًا متوقعًا أقل من (5)، وبلغ الحد الأدنى للتكرار المتوقع (13.76)، مما يشير إلى ملاءمة البيانات لاستخدام اختبار كاي تربيع.

شكل (4) توزيع استجابات أفراد العينة حول مستوى الامتثال التنظيمي الأمني وفق وجود قسم مختص بالأمن السيبراني بالمنشآت الصناعية السعودية



6. الخاتمة ومناقشة النتائج:

هدفت الدراسة إلى التعرف على مستوى تكامل الأمن الفيزيائي والرقمي في المنشآت الصناعية السعودية، والكشف عن طبيعة العلاقة بين وجود قسم مختص بالأمن السيبراني ومستوى الامتثال الأمني، مع تفسير النتائج في ضوء التوجهات الاستراتيجية لرؤية المملكة العربية السعودية 2030. وقد أظهرت النتائج الوصفية أن ممارسات التكامل بين الأمن الفيزيائي والرقمي جاءت بوجه عام ضمن المستوى المتوسط، وهو ما يشير إلى وجود تطبيق لممارسات التكامل في المنشآت محل الدراسة، إلا أن هذا التطبيق لم يصل إلى مستويات مرتفعة وفق تقديرات أفراد العينة.

وأظهرت النتائج تفاوتًا نسبيًا بين ممارسات التكامل المختلفة، حيث سجلت عبارة «يوجد تنسيق مستمر بين فرق الأمن الفيزيائي والأمن السيبراني» أعلى متوسط حسابي بين بنود مقياس ليكرت، إذ بلغ (3.03)، مع بقائه ضمن المستوى المتوسط. كما سجلت بعض الممارسات المرتبطة بالوعي والمشاركة التنظيمية والالتزام الأمني متوسطات متقاربة؛ فقد بلغ متوسط عبارة «يمتلك الموظفون وعيًا كافيًا بالمخاطر الأمنية المترابطة» (2.93)، وبلغ متوسط كل من المشاركة في وضع الخطط والاستراتيجيات الأمنية والالتزام باللوائح والتشريعات الأمنية (2.90). وتشير هذه النتائج إلى أن الجوانب التنظيمية والتنسيقية والامتثال الأمني كانت من أكثر الجوانب حضورًا نسبيًا في المنشآت محل الدراسة، وإن بقيت جميعها ضمن المستوى المتوسط. كما أظهرت النتائج الوصفية الخاصة بممارسات الامتثال الأمني أن البنود المتعلقة بالالتزام باللوائح، وتطبيق متطلبات الأمن السيبراني، وتحديث السياسات، وإجراء المراجعات الدورية، ومتابعة الامتثال سجلت جميعها مستويات متوسطة. وبلغ المتوسط الوصفي غير الموزون لمتوسطات البنود المتعلقة بالامتثال الأمني نحو (2.85)، بما يشير إلى أن ممارسات الامتثال موجودة لدى المنشآت محل الدراسة بدرجة متوسطة، مع وجود مجال لتطوير آليات المتابعة والتدقيق والتحديث المستمر للسياسات والمتطلبات الأمنية.

وفيما يتعلق بوجود قسم مختص بالأمن السيبراني، أظهرت النتائج أن 52.6% من أفراد العينة أفادوا بعدم وجود قسم مختص بالأمن السيبراني في منشآتهم، مقابل 47.4% أفادوا بوجود قسم مختص. ويعكس ذلك تقاربًا نسبيًا بين المجموعتين، مع ارتفاع طفيف في نسبة المنشآت التي لا يتوافر فيها قسم متخصص، وهو ما قد يشير إلى تنوع النماذج التنظيمية المستخدمة في إدارة وظائف الأمن السيبراني بين المنشآت الصناعية. أما فيما يتعلق بالعلاقة بين وجود قسم مختص بالأمن السيبراني ومستوى الامتثال الأمني، فقد أظهرت نتائج اختبار كاي تربيع عدم وجود علاقة ذات دلالة إحصائية بين المتغيرين، حيث بلغت قيمة كاي تربيع لبيرسون ($\chi 2$ =1.094) عند درجات حرية (4)، وبمستوى دلالة بلغ (p=0.895)، وهو أكبر من مستوى الدلالة المعتمد (0.05). كما بلغت قيمة معامل Cramer's V نحو (0.071)، مما يشير إلى أن قوة العلاقة بين المتغيرين ضعيفة جدًا.

وتعني هذه النتيجة أن البيانات المتاحة لا تقدم أدلة إحصائية كافية على اختلاف مستوى الالتزام باللوائح والتشريعات الأمنية باختلاف وجود قسم مختص بالأمن السيبراني من عدمه. ولا ينبغي تفسير ذلك على أن وجود قسم متخصص ليست له أهمية أمنية، وإنما يشير إلى أن مجرد الوجود التنظيمي الرسمي للقسم لم يكن، في هذه العينة، عاملًا مميزًا لمستوى الامتثال التنظيمي الأمني. فقد تنفذ بعض المنشآت وظائف الأمن السيبراني من خلال إدارات تقنية أو فرق مشتركة أو جهات خارجية دون إنشاء قسم مستقل، كما أن وجود قسم متخصص لا يضمن بالضرورة ارتفاع مستوى الامتثال إذا لم يصاحبه نضج في السياسات والإجراءات وآليات التدقيق والمتابعة والتنسيق المؤسسي.

كما تدعم التحليلات الاستكشافية المتعلقة ببعض ممارسات التكامل هذا التفسير؛ إذ لم تظهر علاقات ذات دلالة إحصائية بين وجود قسم مختص بالأمن السيبراني وكل من مراقبة الأحداث الأمنية المتكاملة والتنسيق الأمني المستمر. وتشير هذه النتائج مجتمعة إلى أن

الهيكل التنظيمي وحده قد لا يكون كافيًا لتفسير مستوى التكامل أو الامتثال الأمني، وأن الممارسات الفعلية، ومستوى النضج الأمني، ووضوح المسؤوليات، وتكامل الأنظمة والسياسات، وآليات التنسيق والتدقيق قد تكون أكثر أهمية من مجرد وجود وحدة تنظيمية مستقلة.

1.6. مناقشة النتائج في ضوء رؤية المملكة العربية السعودية 2030

يمكن تفسير النتائج الوصفية للدراسة في ضوء توجهات رؤية المملكة العربية السعودية 2030 المرتبطة بالتحول الرقمي، وتعزيز الأمن السيبراني، ورفع الكفاءة والجاهزية المؤسسية، وتطوير الحوكمة في القطاعات الحيوية والصناعية. وقد تضمنت الاستبانة عددًا من العبارات ذات الصلة بهذه التوجهات، وأظهرت النتائج أن تقديرات أفراد العينة تجاه الإسهامات الاستراتيجية للتكامل الأمني جاءت جميعها ضمن المستوى المتوسط.

فقد بلغ متوسط الاستجابة لعبارة «يسهم التكامل بين الأمن الفيزيائي والرقمي في دعم التحول الرقمي» (2.67)، وبلغ متوسط عبارة «يساعد التكامل الأمني على تعزيز جاهزية المنشآت الصناعية للمستقبل» (2.84)، في حين بلغ متوسط عبارة «يساهم التكامل الأمني في رفع مستوى الحوكمة والامتثال» (2.73). كما بلغ متوسط الاستجابة لعبارة «يدعم التكامل الأمني تحقيق مستهدفات الأمن السيبراني الوطنية» (2.79)، وبلغ متوسط عبارة «يساهم التكامل الأمني في تعزيز تنافسية المنشآت الصناعية السعودية» (2.69). وبلغ المتوسط الوصفي العام لهذه المجموعة من العبارات نحو (2.74)، وهو ضمن المستوى المتوسط.

وتشير هذه النتائج إلى أن أفراد العينة يدركون بدرجة متوسطة الصلة بين تكامل الأمن الفيزيائي والرقمي وبين عدد من التوجهات الاستراتيجية المرتبطة بالتحول الرقمي، والجاهزية، والحوكمة، والأمن السيبراني الوطني، والتنافسية الصناعية. ومع ذلك، فإن بقاء هذه التقديرات ضمن المستوى المتوسط يشير إلى وجود فرصة لتعزيز توظيف التكامل الأمني بصورة أكثر نضجًا داخل المنشآت الصناعية، بما يدعم بناء بيئات تشغيلية أكثر ترابطًا وقدرة على التعامل مع المخاطر الفيزيائية والرقمية المتداخلة.

ولا تعني هذه النتائج أن الدراسة أثبتت إحصائيًا تحقيق مستهدفات رؤية المملكة 2030، إذ لم تعامل الرؤية بوصفها متغيرًا إحصائيًا مستقلاً أو تابعًا، وإنما تم توظيفها إطارًا استراتيجيًا لتفسير دلالات النتائج. ومن هذا المنظور، يمكن القول إن المستوى المتوسط لممارسات التكامل والامتثال الذي أظهرته الدراسة يعكس وجود قاعدة قائمة يمكن البناء عليها، في مقابل حاجة مستمرة إلى تطوير التكامل التقني والتنظيمي، وتعزيز التنسيق والحوكمة والامتثال، بما يتوافق مع التوجه العام نحو التحول الرقمي ورفع الجاهزية المؤسسية في القطاع الصناعي السعودي.

وفي ضوء ذلك، تخلص الدراسة إلى أن تكامل الأمن الفيزيائي والرقمي يمثل مجالًا مهمًا لتطوير الممارسات الأمنية في المنشآت الصناعية، إلا أن النتائج الفعلية لا تبرر وصفه بأنه حقق أثرًا إحصائيًا مثبتًا على الامتثال الأمني. كما توضح النتائج أن وجود قسم مستقل للأمن السيبراني لا يرتبط، وفق البيانات الحالية، بمستوى أعلى من الامتثال التنظيمي الأمني، مما يؤكد أهمية النظر إلى الأمن السيبراني والتكامل الأمني بوصفهما منظومة من السياسات والممارسات والقدرات والتنسيق المؤسسي، وليس مجرد وجود وحدة تنظيمية متخصصة.

2.6. ملخص نتائج الدراسة:

- أظهرت النتائج أن مستوى تكامل الأمن الفيزيائي والرقمي في المنشآت الصناعية السعودية جاء بوجه عام ضمن المستوى المتوسط، حيث تراوحت متوسطات بنود مقياس ليكرت بين (2.67–3.03).

- بلغ المتوسط الوصفي العام لممارسات التكامل في البنود المرتبطة بالجوانب التقنية والتنظيمية والتدريبية نحو (2.83)، وهو ما يعكس مستوى متوسطًا من تطبيق ممارسات التكامل بين الأمن الفيزيائي والرقمي.
- سجل التنسيق المستمر بين فرق الأمن الفيزيائي والأمن السيبراني أعلى متوسط بين بنود الاستبانة بلغ (3.03)، مع بقائه ضمن مستوى الاستجابة المتوسط.
- أظهرت ممارسات الامتثال الأمني مستوى متوسطًا بوجه عام، وبلغ المتوسط الوصفي لبنود الامتثال الأمني نحو (2.85)، كما بلغ متوسط الالتزام باللوائح والتشريعات الأمنية (2.90).
- أظهرت النتائج أن 47.4% من أفراد العينة أفادوا بوجود قسم مختص بالأمن السيبراني في منشآتهم، في مقابل 52.6% أفادوا بعدم وجود قسم مختص.
- لم يظهر اختبار كاي تربيع وجود علاقة ذات دلالة إحصائية بين وجود قسم مختص بالأمن السيبراني ومستوى الامتثال الأمني، حيث بلغت قيمة Pearson Chi-Square ($\chi^2 = 1.094$، $df = 4$، $p = 0.895$)، وهي قيمة غير دالة إحصائيًا عند مستوى (0.05).
- أظهرت قيمة Cramer's V ≈ 0.071 أن قوة العلاقة بين وجود قسم مختص بالأمن السيبراني ومستوى الامتثال الأمني كانت ضعيفة جدًا.
- وبناءً على النتيجة السابقة، لم تتوافر أدلة إحصائية كافية لدعم الفرضية التي تفترض وجود علاقة ذات دلالة إحصائية بين وجود قسم مختص بالأمن السيبراني ومستوى الامتثال الأمني في المنشآت الصناعية السعودية.
- أظهرت التحليلات الاستكشافية عدم وجود علاقات ذات دلالة إحصائية بين وجود قسم مختص بالأمن السيبراني وكل من مراقبة الأحداث الأمنية المتكاملة ($p=0.832$) والتنسيق الأمني المستمر ($p=0.868$).
- جاءت تقديرات أفراد العينة للعبارات المرتبطة بالإسهامات الاستراتيجية للتكامل الأمني في دعم التحول الرقمي، والجاهزية المستقبلية، والحوكمة والامتثال، ومستهدفات الأمن السيبراني الوطنية، والتنافسية الصناعية ضمن المستوى المتوسط، بمتوسط وصفي عام بلغ نحو (2.74).
- تشير النتائج في ضوء رؤية المملكة العربية السعودية 2030 إلى وجود مستوى متوسط من الممارسات المرتبطة بالتكامل الأمني والتحول الرقمي والجاهزية والحوكمة، بما يعكس وجود أساس يمكن تطويره وتعزيز نضجه في المنشآت الصناعية، دون اعتبار رؤية 2030 متغيرًا إحصائيًا تم اختباره في الدراسة.

3.6. التوصيات:

- تعزيز مستوى التكامل التقني والتنظيمي بين الأمن الفيزيائي والأمن الرقمي في المنشآت الصناعية، من خلال تطوير أنظمة وإجراءات أمنية مترابطة تدعم تبادل المعلومات والتنسيق بين مختلف الوظائف الأمنية.
- تطوير السياسات والإجراءات المشتركة بين فرق الأمن الفيزيائي والأمن السيبراني بما يسهم في توضيح المسؤوليات، وتعزيز التنسيق المستمر، وتقليل الازدواجية في المهام والإجراءات الأمنية.
- التركيز على نضج ممارسات الأمن السيبراني والامتثال، وعدم الاكتفاء بوجود قسم مختص بالأمن السيبراني، وذلك من خلال تعزيز آليات الحوكمة والمتابعة والتدقيق وقياس مستوى الالتزام بالمتطلبات الأمنية.
- تعزيز برامج التدريب والتوعية المشتركة للعاملين في مجالات الأمن الفيزيائي والأمن السيبراني وإدارة المخاطر، بما يرفع مستوى الوعي بالمخاطر المترابطة ويحسن القدرة على التعامل مع الحوادث الأمنية المشتركة.

- تطوير آليات دورية لمتابعة الامتثال الأمني تشمل تحديث السياسات وفق المتطلبات النظامية، وإجراء المراجعات والتدقيقات الأمنية، ومتابعة الالتزام باللوائح والتشريعات والمتطلبات المعتمدة.
- دعم توظيف التقنيات الحديثة في المراقبة والتحليل الأمني، بما في ذلك المنصات الموحدة وأنظمة المراقبة الذكية وتحليل البيانات، بما يساعد على تحسين اكتشاف الأحداث الأمنية وسرعة الاستجابة لها، مع تقييم ملاءمة هذه التقنيات لاحتياجات كل منشأة.
- تطوير أطر متكاملة لإدارة المخاطر الأمنية تجمع بين البيانات والمخاطر الفيزيائية والرقمية، بما يدعم دقة تقييم المخاطر واتخاذ القرارات الأمنية على أساس أكثر شمولًا.
- تعزيز التعاون بين المنشآت الصناعية والجهات التنظيمية ذات العلاقة في تبادل الخبرات وتطبيق أفضل الممارسات في مجالات التكامل الأمني والامتثال، بما يدعم التوجهات المرتبطة بالتحول الرقمي والحوكمة والجاهزية والأمن السيبراني في ضوء رؤية المملكة العربية السعودية 2030.

7. المراجع:

1.7. المراجع العربية:

مهران، أسماء جابر علي. (2024). الانعكاسات والمخاطر الاجتماعية للجرائم والهجمات السيبرانية على الأمن الرقمي وآليات المواجهة في ضوء رؤية مصر 2030. مجلة الأمن القومي والاستراتيجية، 2(4)، 88–103. https://doi.org/10.21608/nsas.2024.362423

خشبة، محمد ماجد، والريس، أماني حلمي، والجوهري، عصام، وإبراهيم، داليا أحمد، وجمال الدين، هبة، وربيع، حسن محمد. (2021). الأبعاد التنموية والاستراتيجية للأمن السيبراني ودوره في دعم الاقتصادات الرقمية والمشفرة: مسارات التجربة المصرية في ضوء التجارب العالمية (سلسلة قضايا التخطيط والتنمية، رقم 326). معهد التخطيط القومي. https://repository.inp.edu.eg/items/96414d87-1772-4b43-a0a7-dd2fc1d9d504

2.7. المراجع الأجنبية:

Gamage, A. N. K. K. (2025). Research design, philosophy, and quantitative approaches in scientific research methodology. Scholars Journal of Engineering and Technology, 13(2), 91–103. https://doi.org/10.36347/sjet.2025.v13i02.004

Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. Applied Sciences, 8(6), 898. https://doi.org/10.3390/app8060898

Haj Ahmad, K., & Taha, A.-E. M. (2026). Laying the digital foundation: Enforcing minimum Industry 4.0 standards for new SME factories in Saudi Arabia. Sustainability, 18(6), 3122. https://doi.org/10.3390/su18063122

Miskini, M. S. (2026). Digital supply chain transformation in Saudi industrial manufacturing under Vision 2030. Veredas do Direito, 23(9), e236678. https://doi.org/10.18623/rvd.v23.6678

Abdullah, M., Nawaz, M. M., Saleem, B., Zahra, M., Ashfaq, E. B., & Muhammad, Z. (2025). Evolution cybercrime—Key trends, cybersecurity threats, and mitigation strategies from historical data. Analytics, 4(3), 25. https://doi.org/10.3390/analytics4030025

Agrawal, N., & Kumar, R. (2022). Security perspective analysis of industrial cyber physical systems (I-CPS): A decade-wide survey. ISA Transactions, 130, 10–24. https://doi.org/10.1016/j.isatra.2022.03.018

Staffenova, N., Dupakova, D., & Kubina, M. (2026). Integration of ISMS into the organization's strategy and its impact on security culture in the digital environment. Administrative Sciences, 16(1), 26. https://doi.org/10.3390/admsci16010026

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). An integrated outlook of cyber–physical systems for Industry 4.0: Topical practices, architecture, and applications. Green Technologies and Sustainability, 1(1), 100001. https://doi.org/10.1016/j.grets.2022.100001

Alhussain, S. (2026). The environmental impact of cloud computing in Saudi Arabia and its role in achieving Vision 2030 goals. Green Technologies and Sustainability, 4(3), 100415. https://doi.org/10.1016/j.grets.2026.100415

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2022). Employees' intentions toward complying with information security controls in Saudi Arabia's public organisations. Government Information Quarterly, 39(4), 101721. https://doi.org/10.1016/j.giq.2022.101721

Zaid, T., & Garai, S. (2024). Emerging trends in cybersecurity: A holistic view on current threats, assessing solutions, and pioneering new frontiers. Blockchain in Healthcare Today, 7(1). https://doi.org/10.30953/bhty.v7.302

Clemmensen, T., Tourchi Moghaddam, M., & Nørbjerg, J. (2025). Cyber-physical systems with human-in-the-loop: A systematic review of socio-technical perspectives. Journal of Systems and Software, 226, 112348. https://doi.org/10.1016/j.jss.2025.112348

Doi: https://doi.org/10.52133/ijrsp.v7.81.5