Journal of Economic, Administrative and Legal Sciences (JEALS) • Vol 9, Sup Issue 9 (2025) • P: 26 - 1
https://journals.ajsrp.com/index.php/jeals
ISSN: 2522-3372 (Online) • ISSN: 2522-3372 (Print)

The Reality of Sustainability of Emerging Cybersecurity Companies in Light of Individuals' Attitudes in Saudi Society

Eng. Mohammad Abdulaziz Alduriweesh
Midocean University | KSA

Received: 03/04/2025
Revised: 13/04/2025
Accepted: 15/06/2025
Published: 30/09/2025

* Corresponding author: m_al_duriweesh@hotmail.com

Citation: Alduriweesh, M. A. (2025). The Reality of Sustainability of Emerging Cybersecurity Companies in Light of Individuals' Attitudes in Saudi Society. *Journal of Economic, Administrative and Legal Sciences, 9*(9S), 1 – 26. https://doi.org/10.26389/AJSRP.D050425

Abstract: The study aimed to explore the reality of sustainability of emerging cybersecurity companies in the Kingdom of Saudi Arabia in light of individuals' attitudes within Saudi society, with a focus on the importance of these companies in data protection and the provision of digital security solutions. To achieve the study's objectives, a descriptive methodology was adopted using a survey approach. Data was collected through a questionnaire distributed to a sample of 250 individuals, divided into two groups: the first group included 170 employees working in emerging cybersecurity companies at both administrative and technical levels, while the second group consisted of 80 beneficiaries of these companies' services within Saudi society. Using this sample, the study analyzed the attitudes of both groups and their level of trust in the sustainability of these companies. The results based on the study's hypotheses indicated a strong relationship between individuals' attitudes toward cybersecurity and the extent to which emerging companies apply security standards and policies, which directly contributes to the growth and sustainability of this vital sector in the Kingdom. In light of these findings, the study recommends enhancing public awareness of cybersecurity, investing in the development of human capital, updating legislation in line with technological advancements, and fostering an entrepreneurial environment to support the cybersecurity sector in the Kingdom of Saudi Arabia.

Keywords: Cybersecurity, Startups, Sustainability, Public Awareness, Saudi Society.

واقع استدامة شركات الأمن السيبراني الناشئة في ضوء توجهات الأفراد في المجتمع السعودي

م. محمد عبد العزيز الدريويش
جامعة ميدأوشن | المملكة العربية السعودية

المستخلص: هدفت الدراسة إلى استكشاف واقع استدامة شركات الأمن السيبراني الناشئة في المملكة العربية السعودية في ضوء توجهات الأفراد في المجتمع السعودي، مع التركيز على مدى أهمية هذه الشركات في مجال حماية البيانات وتقديم الحلول الأمنية الرقمية. ولتحقيق أهداف الدراسة، تم اتباع المنهج الوصفي باستخدام الأسلوب المسحي، حيث تم جمع البيانات باستخدام استبانة موجهة إلى عينة مكونة من (250) فردًا، موزعين على فئتين: الأولى تضم (170) من العاملين في شركات الأمن السيبراني الناشئة، من مستويات إدارية وفنية. أما الفئة الثانية فتمثلت في (80) من المستفيدين من خدمات هذه الشركات داخل المجتمع السعودي. وباستخدام هذه العينة، تم تحليل توجهاتهم هذه الفئات ومدى ثقتهم في استدامة هذه الشركات. وأوضحت النتائج المترتبة على فرضيات الدراسة إلى وجود علاقة قوية بين توجهات الأفراد نحو الأمن السيبراني، ومدى تطبيق الشركات الناشئة للمعايير والسياسات الأمنية، مما يسهم بشكل مباشر في نمو واستدامة هذا القطاع الحيوي في المملكة. وفي ضوء النتائج توصي الدراسة بضرورة تعزيز الوعي المجتمعي بالأمن السيبراني، والاستثمار في تنمية رأس المال البشري، وتحديث التشريعات بما يتماشى مع التطورات التقنية وتعزيز بيئة ريادة الأعمال لدعم قطاع الأمن السيبراني في المملكة العربية السعودية.

الكلمات المفتاحية: الأمن السيبراني، الشركات الناشئة، الاستدامة، وعي الأفراد، المجتمع السعودي.

أولاً: مقدمة:

في ظل التحول الرقمي المتسارع، باتت الشركات الصغيرة والمتوسطة تعتمد بشكل متزايد على التقنيات الرقمية لتعزيز كفاءتها التشغيلية وتوسيع نطاق أعمالها. إلا أن هذا الاعتماد المتزايد جعلها أكثر عرضة الهجمات السيبرانية، مثل اختراق البيانات، وهجمات برامج الفدية، وهجمات التصيد الاحتيالي. وتزداد تعقيداتها مع ازدياد حجم البيانات واستدامة اعتماد الشركات الأمن السيبراني على الأنظمة الإلكترونية. وعلى الرغم من الأهمية المتزايدة لتأمين البنية الرقمية، لا تزال العديد من هذه المؤسسات تُظهر مستويات منخفضة من الوعي والاستعداد لمواجهة تلك التهديدات السيبرانية، التي تتنوع بين اختراقات البيانات وهجمات برامج الفدية والتصيد الاحتيالي، ما يضع هذه المؤسسات أمام تحديات متنامية تتعلق بالأمن الرقمي واستدامته (آل مداوي، 2023، 15-16).

وفي هذا السياق، يتجلى الاعتماد المجتمعي الكبير على الإنترنت، وتزايد الثقة الممنوحة من قبل الأفراد في الشركات الحكومية والأهلية في تسليم بياناتهم الشخصية والحساسة لأفراد المجتمع؛ لتلبية احتياجاتهم المختلفة وهو من جانب آخر يعكس لنا المخاطر المحتملة التي قد تنتج من تعاملنا واعتمادنا اللامحدود على تكنولوجيا المعلومات، وهو ما يبرز الحاجة إلى رفع الوعي المجتمعي بأهمية الأمن السيبراني في المجتمع السعودي، ليس فقط على مستوى الفرد، بل على مستوى المجتمع ككل، إذ يعكس هذا الوعي عنصرًا أساسيًا في حماية البنية التحتية الرقمية الوطنية، والمحافظة على أمن الأفراد وخصوصياتهم.

وتتعاظم أهمية هذا البحث من تركيزه على شركات الأمن السيبراني الناشئة التي تمثل عنصرًا حيويًا في المنظومة الرقمية السعودية، خاصة في ظل التوسع في تقديم الخدمات الرقمية. إذ يتمثل الهدف الرئيسي في تحليل واقع استدامة شركات الأمن السيبراني الناشئة، ونودع لديها كافة معلوماتنا الشخصية والحساسة وكافة ممتلكاتنا؛ لتساهم معنا بالحفاظ على أمن هذه المعلومات والممتلكات من الانتهاكات المتنوعة. كما أنه يهدف البحث إلى تقديم تحليل نقدي متكامل لمشكلة استدامة شركات الأمن السيبراني الناشئة في السعودية، بدءًا من التحديات العامة التي يشهدها القطاع الرقمي عالميًا، مرورًا بتأثيرها على بيئة الشركات الناشئة، وصولاً إلى تحليل العوامل الخاصة التي تؤثر على استمرارية هذه الشركات في ظل البيئة التنظيمية والتنافسية المحلية، ودور توجهات الأفراد في دعمها أو الحد من تطورها.

ويهدف هذا البحث إلى تقديم قراءة تحليلية نقدية للواقع الفعلي لشركات الأمن السيبراني الناشئة، والبحث في مدى توافقها مع تطلعات المجتمع السعودي وثقته بها، كما يستعرض المشكلات التي تحد من نمو هذه الشركات ويقترح حلولًا استراتيجية قابلة للتطبيق لتعزيز استدامتها ضمن إطار رؤية المملكة 2030 للتحول الرقمي.

ثانياً: مشكلة الدراسة:

شهد العالم خلال العقود الأخيرة تحولات جذرية في بنية الاتصالات والمعلومات، مما جعله أقرب إلى "قرية كونية" تتداخل فيها الثقافات والمعلومات، ويزداد فيها اعتماد الأفراد والمؤسسات على الوسائل التقنية الحديثة في مختلف جوانب الحياة. هذا التوسع الرقمي الذي تمخض عن الثورة التكنولوجية لم يكن دائمًا ذا طابع إيجابي، فقد رافقته تحديات ومخاطر مستجدة، من أبرزها التهديدات السيبرانية التي تطال الأفراد والمؤسسات على حد سواء (عبد العزيز، 2012، ص. 38). وفي هذا السياق تُعد المملكة العربية السعودية من الدول التي شهدت تطورًا ملحوظًا في مجال التحول الرقمي، حيث ارتفع عدد مستخدمي الإنترنت إلى نحو 36.31 مليون مستخدم بحلول عام (2024) تبلغ36.31 مليون مستخدم بمعدل إنشار 99.0%، بينما كانت نسبة مستخدمي الإنترنت في عام (2016)، 24 مليون مستخدم وتُشير هذه الأرقام إلى تنامي الاعتماد على التقنيات الرقمية بين أفراد المجتمع السعودي، سواء على مستوى الأفراد أو المؤسسات الناشئة. (هيئة الاتصالات والفضاء والتقنية، التقرير السنوي: 2023)، ويري الباحث وهذا يعكس لنا مدي اعتماد الأفراد والشركات الناشئة على استخدام التقنية؛ لتسهيل التواصل كالتعاملات وتسهيل حياة الأفراد في المجتمع السعودي.

إلا أن هذا التحول المتسارع ترافق مع تزايد الهجمات السيبرانية، التي شكلت ضغطًا متزايدًا على البنية التحتية الرقمية، ما دفع الجهات الحكومية والخاصة إلى تطوير استراتيجيات وسياسات تهدف إلى حماية البيانات، وتعزيز الأمن السيبراني ضمن رؤية المملكة 2030 (الكتاب السنوي للتنافسية العالمية، 2022). ومع ارتفاع القيمة السوقية المتوقعة لقطاع الأمن السيبراني في المملكة من 3.6 مليار دولار في عام 2020 إلى نحو 9.8 مليار دولار في عام 2026 (Forbes Middle East، 2022)، يصبح من الضروري النظر في مدى استدامة شركات الأمن السيبراني الناشئة، ودورها في دعم البنية الأمنية الرقمية للمملكة.

وتُظهر الدراسات الحديثة أن الشركات الناشئة والصغيرة تُعد من أكثر الفئات عرضة للهجمات السيبرانية؛ إذ أن 43% من هذه الهجمات تستهدف الشركات الصغيرة والمتوسطة (Sarker et al., 2021)، كما أن 28% من حالات اختراق البيانات في عام 2020 طالت هذه الفئة تحديدًا. ويعزى ذلك إلى معوقات متعددة أبرزها: نقص التمويل، وغياب الكفاءات البشرية المؤهلة، وقلة الوعي بمخاطر التهديدات الإلكترونية (Atoum & Otoom, 2017؛ Shojaifar & Järvinen, 2021).

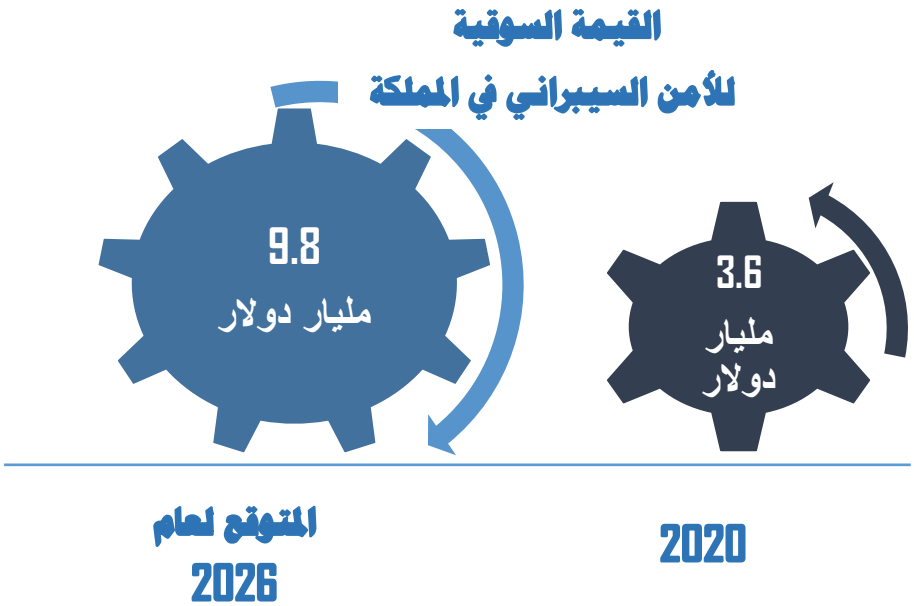
ورغم الجهود التي تبذلها بعض الجهات الحكومية والخاصة من خلال إطلاق برامج توعية ومبادرات تدريبية (Rea-Guaman et al., 2020)، إلا أن هذه المبادرات غالبًا ما تفتقر إلى التخصيص وتستند إلى استراتيجيات عامة لا تلائم الخصوصية الهيكلية والتشغيلية لهذه الشركات، مما يُضعف أثرها على الواقع العملي (Shojaifar et al., 2020). وتُشير بعض الدراسات إلى تدني مستوى الحوكمة الرقمية داخل هذه المؤسسات (آل مداوي، 2023)، مع تدنٍ واضح في تقدير المخاطر السيبرانية (Armenia et al., 2021; Benz & Chatterjee, 2020)، مما ينعكس سلبًا على أداء تلك المؤسسات واستدامتها.

وفي ظل البيئة الرقمية المعقدة التي تتطلب تبني نماذج أمنية مرنة وفعّالة، يبدو واضحًا أن كثيرًا من الشركات الناشئة تفتقر إلى نظم فعالة لقياس الأداء بناءً على معايير الفعالية والكفاءة والإنتاجية والإبداع (عادل ويعقوب، 2022؛ الشريفي، 2019)، وهي معايير ترتبط ارتباطًا وثيقًا بتحقيق الميزة التنافسية في بيئة العمل العالمية (خالد ويعقوب، 2021).

من هنا، تبرز مشكلة الدراسة في تسليط الضوء على واقع استدامة شركات الأمن السيبراني الناشئة في المملكة العربية السعودية، وذلك في ظل توجهات الأفراد في المجتمع السعودي نحو تقنيات الأمن السيبراني وخدماته، ومدى قدرة هذه الشركات على مواكبة التطورات التكنولوجية والتحديات الأمنية المتصاعدة، وتطبيق معايير الأداء والاستدامة بما يضمن لها البقاء والنمو والمساهمة الفعالة في تحقيق الأمن الرقمي الوطني.

وقد شهدت السنوات الأخيرة استغلالاً غير مسبق لشبكات المعلومات والإنترنت، وذلك نظراً لتوافر هذه التقنية وسهولة الحصول عليها وقلة تكاليفها، وإمكانية التخفي والعمل بحرية تامة من خلالها باعتبارها من أكثر وسائل الاتصالات أماناً وانتشاراً (البلادي، وعثمان، 2023، 1 :16).

بالرغم من التقدم التقني، إلا أن العديد من شركات الأمن السيبراني الناشئة، تواجه تحديات كبيرة في تصميم وتطبيق نماذج أمنية فعّالة تتناسب مع طبيعة هذه المؤسسات. فالأطر الحالية غالبًا ما تُبنى لتناسب الشركات الكبرى التي تمتلك موارد مالية وبشرية واسعة، مما يجعل من الصعب على الشركات الناشئة تطبيقها دون الاستعانة بخبراء خارجيين وتحمل تكاليف باهظة، وهو ما قد يُضعف استدامة خدمات هذه الشركات في المجتمع السعودي. أصبحت قضايا الأمن السيبراني من الأولويات الاستراتيجية لاستمرارية حماية البنية التحتية الحيوية لأفراد المجتمع السعودي.



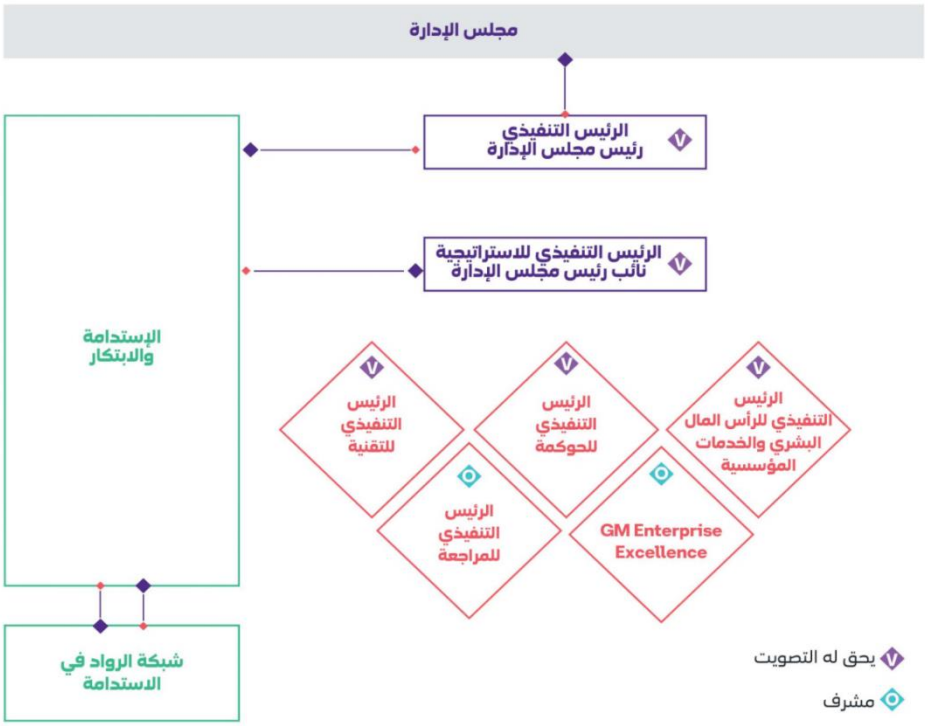
الشكل رقم (1) تقرير خاص Forbes الشركات الأكثر ابتكاراً في السعودية

يوضح الرسم البياني السابق النمو المتوقع للقيمة السوقية لقطاع الأمن السيبراني داخل المملكة العربية السعودية خلال الفترة من عام 2020 إلى 2026. وقد بلغت القيمة السوقية للأمن السيبراني في عام 2020 نحو 3.6 مليار دولار، في حين يُتوقع أن ترتفع هذه القيمة إلى 9.8 مليار دولار بحلول عام 2026، مما يعكس زيادة بنسبة 172% تقريبًا خلال ست سنوات (تقرير خاص Forbes Middle East, 2022).

ووفقًا لبحث أجرته شركة سيمانتك في عام 2016، فإن 43% من الهجمات السيبرانية تستهدف الشركات الصغيرة والمتوسطة، مما يبرز المخاطر المرتبطة بذلك. كما أشار (Sarker et al., 2021) بالإضافة إلى ذلك، أشار تقرير بيانات الأمن السيبراني المدعوم بالذكاء الاصطناعي إلى أن 28% من حالات اختراق البيانات في عام 2020 كانت تشمل الشركات الصغيرة ذات الصلة، مما يوضح استمرارية المشكلة. وقد لاحظ

العديد من الباحثين أيضًا صعوبات متعددة تواجه الشركات الصغيرة والمتوسطة في تنفيذ سياسة أمن سيبراني فعّالة، مثل نقص التمويل، وعدم توفر الموارد البشرية المؤهلة، وعدم الوعي بالتهديدات (Atoum & Otoom, 2017; Shojaifar & Järvinen, 2021).

سعيًا لتعزيز استدامة الأمن السيبراني لدى الشركات الناشئة، تم تنفيذ عدد من المبادرات التي تهدف إلى رفع الوعي وتقديم برامج تدريبية موجهة، حيث أطلقت بعض الجهات الحكومية والخاصة حملات تهدف إلى تعريف أصحاب تلك الشركات بالإجراءات الأساسية لحماية بياناتهم الرقمية (Rea-Guaman et al., 2020). ومع ذلك، غالبًا ما تكون هذه المبادرات محدودة التأثير، لأنها تعتمد على استراتيجيات عامة لا تأخذ بعين الاعتبار الخصائص الفريدة لهذه الفئة من المؤسسات. ومن هنا تبرز الحاجة الملحة إلى تطوير حلول أمن سيبراني أكثر تخصيصًا وفعالية تلائم احتياجات المؤسسات الصغيرة والمتوسطة على وجه التحديد (Shojaifar et al., 2020).



شكل رقم (2) استراتيجية (GROW) الخاصة بحوكمة الاستدامة

(تقرير الاستدامة، 2023، 62)

يُعد الاعتماد على نماذج فعالة ضرورة استراتيجية لضمان استدامة هذه الشركات وقدرتها على مواجهة المخاطر التقنية والتهديدات السيبرانية المتطورة. وهذا ما أكدت عليه دراسة (Armenia et al., 2021; Benz & Chatterjee, 2020) أنه على الرغم من هذا الاهتمام المتزايد، تواجه الشركات الأمن السيبراني الناشئة والمتوسطة مجموعة من التحديات بسبب قلة الموارد والمعرفة المحدودة. فقد أظهرت الدراسة أن غالبية الشركات الصغيرة تظهر تقديرًا منخفضًا للمخاطر السيبرانية، مما يؤدي إلى ضعف الحماية لديها. كما أكدت أيضاً دراسة آل مداوي في إطار محاولة تسليط الضوء على فجوة تطبيق مبادئ الحوكمة في شركات الأمن السيبراني الناشئة، مع التركيز على السياق السعودي الذي يشهد تداخل العوامل التقنية والتنظيمية والاقتصادية (آل مداوي، 2023، 15).

تعد استدامة الأمن السيبراني أمراً حاسماً لضمان الوصول الشامل والجدير بالثقة والمنصف إلى الاتصال. فبينما يُتيح استخدام تكنولوجيا المعلومات والاتصالات (ICT) إدارة أفضل، وزيادة الإنتاجية، فإن استخدام الأنظمة الرقمية يُلد أيضاً مخاطر. من هنا تثير التهديدات السيبرانية والهجمات السيبرانية تحديات أمنية متزايدة باستمرار لكل من القطاعين العام والخاص في جميع البلدان (فتوح، 2021، 5).

ويري الباحث أنه يجث أن تعمل الشركات الناشئة على اقتناص ما تحتويه من فرص لتحولها إلى قيمة لتعزيز أداءها وميزتها التنافسية. لذا أصبحت إدارة الأمن السيبراني ضرورة ملحة للمنظمات التي تسعى لتحسين أداءها وسمعتها وزيادة حصتها السوقية، وبالتالي تحقيق أهدافها الاستراتيجية في بيئة التنافس العالمية بين تلك المنظمات بحيث يغطي الأبعاد الرئيسية لأدائها.

وعليه، يعتبر تقييم أداء الشركات ضرورة ملحة بهدف ضمان تحقيق الأهداف الاستراتيجية للشركة من خلال مضافة مجموعة من مؤشرات الأداء الاستراتيجية والتنفيذية والتي يمكن إجمالها في الفاعلية والكفاءة والإنتاجية والإبداع (عادل، ويعقوب ،2022، والشريفي، (2019) حيث يساهم تحقيق هذه المعايير في تطوير أداء الشركات وتميزها على المستوى المحلي والعالمي وبناء ميزة تنافسية يصعب على المنافسين تجاوزها (خالد، ويعقوب، 2021).

تسعى هذه الدراسة إلى قياس مدى استدامة تطبيق معايير الأمن السيبراني من خلال نموذج مفاهيمي يبحث في العلاقة بين معايير استدامة الأمن السيبراني وأداء شركات الاتصالات الناشئة في السعودية وفقاً لاهم أبعاد قياس أداء الشركات، كما وتسعى هذه الدراسة إلى تسليط الضوء على معايير الأمن السيبراني للباحثين ولمتخذي القرار في شركات الاتصالات الأردنية؛ حيث يُشكل هذا القطاع بيئة اقتصادية خصبة لتطوير آليات تطبيق معايير الأمن السيبراني وفق المعايير العالمية المتقدمة بما يضمن تحقيق أفضل أداء لتلك المنظمات وتعزيز القيمة المضافة لعملائها(ISO 27002 and 27032).

وبسبب تعاظم أهمية أمن المعلومات وأمانها في الأونه الأخيرة، وتفاقم المهددات وكثرة الاختراقات وتواترها على كل الأصعدة وعلى كافة المستويات من الفرد إلى المؤسسات والشركات تعي تدريجياً أخطار الجرائم السيبرانية، وأهمية استدامة شركات الأمن السيبراني على الأمن الاقتصادي والسياسي للسعودية، وعلى المصالح العامة فقد يبدو الإنترنت جنة لمخترقي الشبكات؛ بسبب ظهورهم عليها ظهوراً افتراضياً، وتظهر الإحصاءات الصادرة من هيئة الاتصالات وتقنية المعلومات أن مستخدمي الإنترنت في المملكة العربية السعودية.

على ضوء ما سبق- تتلخص مشكلة الدراسة في: واقع استدامة شركات الأمن السيبراني الناشئة في المملكة العربية السعودية، وذلك في ظل توجهات الأفراد في المجتمع السعودي نحو تقنيات الأمن السيبراني وخدماتها. وقد دفعت هذه التحديات والاعتبارات الباحث إلى إجراء هذه الدراسة، بهدف استكشاف أبعاد المشكلة وتحليلها بعمق، وذلك من خلال السعي للإجابة على التساؤلات التالية:

التساؤل الرئيسي للدراسة فيما يلي:

ما واقع استدامة شركات الأمن السيبراني الناشئة في المملكة العربية السعودية في ضوء توجهات الأفراد في المجتمع السعودي؟

التساؤلات الفرعية:

1- هل توجد فروق ذات دلالة إحصائية في توجهات الأفراد نحو خدمات الأمن السيبراني تُعزى إلى متغيرات ديموغرافية مثل (العمر، الجنس، المستوى التعليمي، ومستوى الاستخدام الرقمي)؟
2- ما مدى تطبيق شركات الأمن السيبراني الناشئة لمعايير الأمن السيبراني وبين الفاعلية التنظيمية لشركة الأمن السيبراني؟
3- إلى أي مدى التزام شركات الأمن السيبراني الناشئة بتطبيق معايير الأمن السيبراني وتحسين الكفاءة التشغيلية؟
4- ما طبيعة العلاقة بين توجهات الأفراد في المجتمع السعودي (ثقتهم، ودوافعهم) واستدامة شركات الأمن السيبراني الناشئة؟

ثالثاً: أهداف الدراسة:

الهدف العام:

تهدف هذه الدراسة إلى التعرف على واقع استدامة شركات الأمن السيبراني الناشئة في المملكة العربية السعودية، من خلال تحليل مدى تأثير توجهات الأفراد في المجتمع السعودي.

الأهداف الفرعية:

1. الكشف عن الفروق في توجهات الأفراد نحو خدمات الأمن السيبراني وفقًا لبعض المتغيرات الديموغرافية (العمر، الجنس، المستوى التعليمي، مستوى الاستخدام الرقمي).
2. دراسة أثر تطبيق معايير الأمن السيبراني والفاعلية التنظيمية لشركات الأمن السيبراني الناشئة.
3. التزام شركات الأمن السيبراني الناشئة بتطبيق معايير الأمن السيبراني وتحسين الكفاءة التشغيلية
4. التعرف على مستوى توجه الأفراد في المجتمع السعودي واستدامة شركات الأمن السيبراني الناشئة.

رابعاً: فروض الدراسة:

تم صياغة الفرضيات الرئيسية والفرعية التالية:

الفرض الرئيسي للدراسة:

توجد علاقة ذات دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين توجهات الأفراد في المجتمع السعودي نحو خدمات الأمن السيبراني، وواقع استدامة شركات الأمن السيبراني الناشئة في المملكة العربية السعودية.

ويشتق من هذه الفرضية الفرضيات الفرعية التالية:

الفرض الأول: توجد فروق ذات دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) في توجهات الأفراد نحو خدمات الأمن السيبراني تُعزى إلى بعض المتغيرات الديموغرافية (العمر، الجنس، المستوى التعليمي، مستوى الاستخدام الرقمي)

الفرض الثاني: توجد علاقة ذات دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين مدى تطبيق معايير الأمن السيبراني، وبين الفاعلية التنظيمية لشركات الأمن السيبراني الناشئة.

الفرض الثالث: توجد علاقة ذات دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين وعي الأفراد، وثقتهم، ودوافعهم لاستخدام خدمات الأمن السيبراني في دعم الكفاءة التشغيلية لشركات الأمن السيبراني الناشئة.

الفرض الرابع: توجد علاقة ذات دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين توجهات الأفراد في المجتمع السعودي، وبين استدامة شركات الأمن السيبراني الناشئة.

خامساً: أهمية الدراسة

تنبع أهمية هذه الدراسة في تقديم تحليل شامل ومتكامل لوضع استراتيجيات فعالة لتحقيق استدامة شركات الأمن السيبراني الناشئة في السعودية، بما يضمن قدرتها على مواجهة التحديات الراهنة والمستقبلية، ويمكن توضيح أهمية هذه الدراسة في النقاط التالية:

1. أن أهمية الشركات الناشئة في مجال الأمن السيبراني تتجاوز مجرد حماية الشركات والأفراد من الهجمات السيبرانية، لتصل إلى المساهمة في النظام البيئي الشامل للأمن السيبراني.
2. تحفيز الابتكار وتعزيز المنافسة في السوق، حيث تلعب الشركات الناشئة دورًا رياديًا في دفع حدود الممكن في مجال الأمن السيبراني، من خلال تقديم حلول غير تقليدية وسريعة التكيّف مع المتغيرات (تقرير Forbes Middl East، 2022).
3. إلهام الشركات الكبرى والجهات الفاعلة المستقرة في السوق لتحسين وتطوير خدماتها باستمرار، بما يواكب مشهد التهديدات المتسارعة والمتطورة، ويعزز من جاهزية المنظومة الأمنية الشاملة.
4. سرعة النمو التي تتميز بها الشركات الناشئة تعد عاملًا حاسمًا، ما يتطلب وجود ضوابط وإجراءات حوكمة فعالة ومبكرة لضمان استمرارية النمو دون حدوث اختلالات هيكلية أو فجوات إدارية.
5. القدرة على جذب رؤوس الأموال والمستثمرين، حيث يعد توفر ممارسات الحوكمة الجيدة والشفافية في العمليات الإدارية من العوامل الجاذبة للمستثمرين، وهو ما يُعد شرطًا مهمًا لتأمين التمويل واستدامة النمو.
6. توافق ممارسات الحوكمة مع تطورات الشركة ودورة حياتها، إذ يجب أن تتطوّر آليات الرقابة والإدارة بشكل يتواكب مع مراحل نمو الشركة وتطلعات المستثمرين، لضمان التوازن بين الابتكار والامتثال التنظيمي.
7. مواجهة صعوبات التأسيس والتوسع في المراحل المبكرة، حيث تواجه الشركات الناشئة تحديًا في مواءمة رؤيتها واستراتيجيتها مع تطلعات المستثمرين، الأمر الذي يتطلب خططًا واضحة وسريعة لتوجيه نماذج الأعمال نحو المسار الصحيح (العطوي، 2021، 732).

سادساً: حدود الدراسة

1. **الحدود البشرية:** اقتصرت الدراسة على عينتين رئيسيتين من الأفراد المرتبطين مباشرة بواقع شركات الأمن السيبراني الناشئة في المملكة العربية السعودية، وهم:
   - العينة الأولى: العاملون في شركات الأمن السيبراني الناشئة (Cipher، CQR، COGNNA) ممن يشغلون مناصب في المستويات الإدارية العليا والوسطى، وكذلك المختصون في الوظائف التقنية والفنية المرتبطة بتطوير وتقديم الخدمات الأمنية.
   - العينة الثانية: مجموعة من أفراد المجتمع السعودي المستفيدين من خدمات هذه الشركات، وذلك بهدف التعرف على توجهاتهم ووعيهم بمستوى الأمان والثقة في استدامة هذه الشركات وخدماتها الرقمية.
2. **الحدود الزمانية:** وهو الإطار الزمني الذي تم خلاله جمع البيانات وتحليلها من العام الأكاديمي **2025–2024م**.
3. **الحدود المكانية:** تم تطبيق الدراسة ميدانيًا على عدد من شركات الأمن السيبراني الناشئة العاملة في المملكة العربية السعودية (شركة Cipher، وشركة CQR، وشركة COGNNA).

سابعاً: المصطلحات والمفاهيم الإجرائية:

1- مفهوم الشركات الناشئة:

حيث بدأ استخدام مصطلح الشركات الناشئة مباشرة بعد الحرب العالمية الثانية، وذلك مع ظهور أولى شركات رس المال الاستثماري، ليشيع استخدام المصطلح بعد ذلك على نطاق واسع.

فمن الناحية اللغوية: تنقسم كلمة Start Up"، بدء التشغيل" إلى قسمين تشكلان جوهر الشركات الناشئة:(Facon)

- " Start ": هو ما يشير إلى وجود فكرة للانطلاق لبدء عمل تجاري جديد؛

:- " U"وهو ما يشير لمرحلة النمو السريع والقوي للأعمال.

ومن الناحية الاصطلاحية: لقد أعطى العديد من الباحثين والكتاب ورواد الأعمال تعريف للشركات الناشئة كل حسب مجاله وتخصصه وخلفيته الفكرية والعلمية وسوف نستعرض هنا مجموعة من هذه التعاريف:

لقد وجد تعريف اصطلاحي للشركات الناشئة في قاموس الفرنسي لاروس Larousse "شركة مبتكرة صغيرة، في قطاع التكنولوجيات الحديثة (Larousse,2021) "

وعرف بول جراهام Paul Graham في مقاله الشهير "الشركة الناشئة = النمو، " STARTUP=GROWTH في سبتمبر 2012 على أن "الشركة الناشئة هي شركة صممت لتنمو بسرعة، وكون الشركة تأسست حديثا لا بجعلها شركة ناشئة، كما أنه من غير الضروري على الشركة الناشئة أن تعمل في قطاع التكنولوجيا أو أن تقبل تمويلا من مخاطر أو مقامر، أو أن يكون لها أي نوع من خطط الخروج، الشيء الوحيد الأساسي هو النمو. وكل شيء آخر تم ربطه بالشركات الناشئة فهو يتبع النمو"(GRAHAM, 2012).

كما إنها تم تعريفها على أنها "مؤسسة بشرية مصممة لإنشاء منتج أو خدمة جديدة في ظل ظروف عدم التيقن الشديد". ويمكن إعطاء مفهوم للشركات الناشئة على أنها "مؤسسة مبدعة مبتكرة، تتمتع بإمكانيات تطور ونمو قوي وسريع لاسيما بفضل قابليتها للتوسع في النموذج كما تسعى هذه الشركات الناشئة إلى طرح وتسويق منتج أو خدمة مبتكرة، أو إيجاد حل لمشكلة ما، وتعمل اغلب هذه الشركات في القطاع التكنولوجي والذكاء الاصطناعي" (GAELLE, 2019).

الشركة الناشئة تود التطور وتكون لديها النية لتكون شركة كبيرة: كما يوضح "ستيف بلانك Steve Blank" أن مدير الشركة الناشئة لا يود فقط أن يكون رئيس نفسه بل يطمح للنمو لأكبر مدى يمكن الوصول إليه، منذ بداية الشركة هناك نية واضحة لتحويلها لشركة عملاقة، ويؤمن مدير الشركة الناشئة أن الفكرة التي لديه هي فكرة عظيمة، سوف تقوم بتغيير المجال الذي يود المنافسة به، وانتزاع العملاء من الشركات المنافسة بل وربما خلق سوق جديد خاص به"(طلعت، 2021).

2- تعريف الأمن السيبراني:

لا شك أن هناك تعريفات كثيرة للأمن السيبراني، سنذكر أهم تلك التعريفات الحديثة؛ فبداية كلمة السيبراني تعني بلغة اللاتينية الفضاء.

أ- تعريف الأمن لغوياً:

مكون من لفظين يعنيان "الأمن: وهو النقيض لكلمة الخوف، والأمن مصدر الفعل أمن أمناً وأماناً وأمنة: أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أمن من الشر، أي سلم منه. قال تعالى فعي كتابعه العزيز: ﴿رَبِ اجْعَلْ هَذَا بَلَداً آمِناً وَارْزُقْ أَهْلَه مِنَ الثَّمَراتِ﴾ (سورة البقرة-126)

ويعرفه الاتحاد الدولي للاتصالات بأنه: "مجموعة من المهمات، مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات وممارسات وتقنيات تستخدم لحماية البيئة السيبرانية والمؤسسات والمستخدمين". (خليل، 2012، 38)

السيبرانية في الاصطلاح:

تعددت التعاريف التي تناولت مصطلح السيبرانية كل حسب الزاوية التي نظر إليها منها، إلا أنها اشتركت في مضمون واحد متقارب في المعنى وهو "استهداف مواقع إلكترونية من خلال وسائل إلكترونية أخرى"، وهي مجموعة من الممارسات التي ترمى إلى حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية أياً كان نوعها، وهذه الممارسات متنوعة إلى تدابير احتياطية استباقية قلب وقوع الخلل، وعلاجية بعد وقلوع الخلل. (الطيار، 2020، 264)

ومفهوم الأمن السيبراني من المفاهيم التي لاقت اهتماماً كبيراً في الآونة الأخيرة نظراً لظهور تقنيات تكنولوجية جديدة، واستخدامها بشكل واقلع في كافة المنشآت، وقد عرف NIST الأمن السيبراني بأنه حماية الأصول المعلوماتية التي تتم من خلال معالجتها وتخزينها ونقلها بواسطة أنظمة المعلومات المتداخلة بين الشريكات الناشئة (NIST, 2018).

ولقد عرفته الوكالة الفرنسية لأمن أنظمة الإعلام ANSSI وهي وكالة مكلفة بالدفاع السيبراني الفرنسي، بأنه فضاء التواصل المشكل من خلال الربط البيني العالمي للمعدات المعالجة الآلية للمعطيات الرقمية، وأنه لا يقتصر ذلك فقط على شبكة الإنترنت، إنما يشمل شبكات عالمية وخاصة مثل (Gps/ AcARs / swift/ psth) (تغريد صفاء وآخرون، 2020،194)، وعرفه الكابتان Lento Martti & Nettaanmaki Pekka فعي كتابهما Automation and technology, Analytics: security cyber بأنه مجموعة من الإجراءات التي تتخذ في الدفاع ضد الهجمات السيبرانية، وعواقبها، وتنفيذ التدابير المضادة المطلوبة(الشمري، 2020، 227). وفي تكوين رؤي حول كيفية تحسين وحوكمة أمن معلومات المنشأة وجهود إدارة المخاطر. (Ramirez, M, Ariza, 2022).

ثامناً: الإطار النظري

1- الإطار النظري للدراسة

أ- نبذة تاريخية عن الأمن السيبراني: (آل مداوي، 2023، 116-117)

1- بداية وضع الأسس الأولى لمكافحة مخاطر الأمن السيبراني كانت مع حلول الثمانينات، وقد أقر الكونجرس أول قانون في العالم لمكافحة الجريمة السيبرانية سنة 1984م، وهو قانون الاحتيال وإساءة استخدام الحاسوب.

2- وأول من استخدم كلمة cyber هو ويليام جيبسون في كتابه الكلاسيكي عام 1984م، وفي يوم 2 نوفمبر 1988م أطلقت موريس- أحد طلاب جامعة كورنيل في الولايات المتحدة الأمريكية - أول دودة حاسوب في تاريخ الإنترنت. وكان إطلاق هذه الدودة هو النقطة الأولى التي بدأ عندها الاهتمام الجدي بكيفية تعزيز الأمن السيبراني. وفي 1989م ظهر فيروس المنتقم الأسود، ويعتبر أول فيروس يحتوي على خصائص العدوى، وظهر في نفس السنة فيروس فرودو مع إمكانية التخفي. ثم أضيفت إليه جهود ستيفنسون عام 1989م؛ ليرسم صورة أقرب إلى الشمولية عن ماهية مفهوم الفضاء الذي يتشارك فيه الناس.

3- وفي عام 1991 م، استخدمت كلمة سايبر مقترنة بالفضاء، وأصبح هذا المفهوم أشمل وأوسع من الإنترنت؛ ليضم كل الاتصالات والشبكات، وقواعد البيانات، ومصادر المعلومات.

4- أما في بداية التسعينات أصبح القراصنة أكثر قوة، وأصبحوا يشاركون الفيروسات فيما بينهم، ومع حلول عام 1995 م ظهر ما يعرف باسم الفيروسات، التي تستهدف الملفات العادية؛ مما يسهل الإيقاع بالضحية. وفي فترة الثورة الرقمية في منتصف العقد الماضي، انتبه الغرب إلى قضية الإرهاب الإلكترونية ومخاطره؛ حيث قام الرئيس الأمريكي السابق بيل كلينتون في عام 1996م بتشكيل لجنة حماية منشآت البنية التحتية الحساسة.

5- عام 2000 م، فقد تطورت هذه الجرائم، ووصلت لنطاق أوسع، وتم استخدام المعلومات في الإرهاب المنظم من خلال ضرب البنى التحتية للدول؛ سواء كانت مرافق عامة أم خدمات، وأيضا البنى العسكرية والاقتصادية المتمثلة في البنوك وغيرها.

6- ومع مطلع عام 2001 م، وبتعاون خبراء مع وزارة العدل الأمريكية - عرفت الوزارة الجريمة السيبرانية.

7- أما المرحلة الثانية من القمة العالمية لمجتمع المعلومات فقد أقيمت في تونس في نوفمبر 2005 م، عَهِدَ قادةُ العالم فيها بأن تكون مسالة تعزيز الأمن السيبراني على رأس جهود التنسيق الدولية.

8- وقد عقدت الهيئةُ المنتدى الدولي للأمن السيبراني في دورته الأولى خلال الفترة 4- 5 فبراير 2020م في مدينة الرياض، تحت شعار (تضافر الجهود نحو عالم سيبراني أفضل). وجاء عقد المؤتمر تزامناً مع رئاسة السعودية لمجموعة العشرين. وقد شهد المنتدى مشاركة 147 متحدثاً من داخل المملكة وخارجها، كما تجاوز عدد الحضور 3500 مشارك.

9- ويعد المنتدى الدولي للأمن السيبراني منصة عالمية تتناول موضوعات الأمن السيبراني وبناء أسس التعاون، تنظمه الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية، وكان انعقاد الدورة الأولى بالتزامن مع رئاسة المملكة لمجموعة العشرين، ويمثل المنتدى منصة تفاعلية عالمية لكافة المعنيين والمختصين بمجال الأمن السيبراني من ممثلي القطاعات الحكومية والخاصة، والمنظمات غير الربحية، والأوساط التعليمية والأكاديمية حول العالم، بهدف نقل المعرفة حول موضوعات الأمن السيبراني، وبناء أسس التعاون بين الدول والمنظمات؛ ليصبح قطاع الأمن السيبراني عنصراً ممكناً في مواجهة التحديات المستقبلية، وصناعة التنمية الاقتصادية والاجتماعية في السعودية وحول العالم.

10- ونظمت الهيئة الوطنية للأمن السيبراني النسخة الثانية من المنتدى الدولي للأمن السيبراني تحت شعار (إعادة التفكير في الترتيبات السيبرانية العالمية)، يومي 9 و10 نوفمبر 2022 في العاصمة الرياض، بمشاركة نخبة من صناع القرار والرؤساء التنفيذيين، وكبار المسؤولين الحكوميين، وممثلي أبرز الشركات العالمية، والمنظمات غير الحكومية، والأوساط الأكاديمية من حول العالم؛ لمناقشة القضايا الاستراتيجية، وفرص التعاون بين الشركاء الدوليين في مجال الأمن السيبراني. وشهد المنتدى انعقاد أكثر من 30 جلسة حوارية، تناولت مجموعة من الموضوعات التي ناقشت آفاق التغيير في المشهد السيبراني، والاقتصادات السيبرانية، والتطور الجيوسيبراني، ومستقبل العمل السيبراني، والأمن السيبراني للجميع. وتطرق المنتدى كذلك إلى أهمية التعاون الدولي وبحث الحلول العملية لسد الفجوة السيبرانية عالمياً، واستكشاف مستقبل الأمن السيبراني، وضمان تحقيق الأمن السيبراني لجميع المجتمعات. (المنيع، 2022)

ب- التحديات التي تواجه شركات الأمن السيبراني الناشئة:

على الرغم من التوجه الحكومي الداعم للاستثمار في القطاع الرقمي، تواجه شركات الأمن السيبراني الناشئة تحديات تتعلق باستدامتها. بسبب المنافسة الشديدة والضغوط المالية والتقنية، لمواكبة التطورات التكنولوجية والحفاظ على القدرة الابتكارية. وتشمل أبرز التحديات ما يلي:

1- التغير التقني والابتكارية المستمرة: إذ يتطلب مواكبة الابتكارات التكنولوجية استثمارات ضخمة في البحث والتطوير، مما يضع ضغوطاً مالية على الشركات الناشئة، حيث يشهد قطاع الأمن السيبراني تطورًا تقنيًا سريعًا، مما يتطلب من الشركات الناشئة القدرة على مواكبة هذا التغير المستمر. إن عدم القدرة على الاستثمار الكافي في البحث والتطوير قد يؤدي إلى تخلف الشركات عن المنافسين الذين يمتلكون بنية تحتية تقنية متقدمة. وقد أشارت التقارير إلى أن الشركات التي تعتمد على الابتكار التقني تحقق معدلات نمو أعلى وتتمتع بقدرة تنافسية أفضل على الصعيدين الوطني والعالمي.

2- نقص الموارد والتمويل: الكثير من الشركات الناشئة تعاني من صعوبات في الحصول على التمويل اللازم، فعلى الرغم من الدعم الوطني وتوفر بعض البرامج التمويلية، إلا أن الكثير من الشركات تعاني من ضعف في السيولة المالية مما يؤثر على قدرتها على توسيع نطاق خدماتها في قطاع الأمن السيبراني وتحديث تقنياتها. (Forbes Middl East, 2022 تقرير)

3- عدم كفاية تبني ثقافة الحوكمة: أن العديد من شركات الأمن السيبراني الناشئة تعاني من ضعف في تطبيق أنظمة الحوكمة الداخلية، مما يؤدي إلى انخفاض الكفاءة الإدارية وتردي الأداء في الأوقات الحرجة. وتبرز الدراسة أهمية بناء ثقافة مؤسسية قوية تستند إلى مبادئ الحوكمة كوسيلة لتجاوز الأزمات وتحقيق النمو المستدام.

4- تحديات الثغرات التنظيمية والتشريعية: تؤثر التعقيدات الإجرائية والاختلافات في تطبيق الأطر التنظيمية على البيئة العملية لهذه الشركات، مما يعيق نموها واستدامتها. وتعتبر الأطر التنظيمية والتشريعية من العوامل المحورية في خلق بيئة آمنة ومستدامة لنمو شركات الأمن السيبراني. ورغم الجهود المبذولة من قبل الجهات الحكومية مثل الهيئة الوطنية للأمن السيبراني لتحديث القوانين وتبسيط الإجراءات، إلا أن الثغرات التنظيمية ما تزال قائمة وتحد من قدرة الشركات على التوسع وتقديم حلول مبتكرة بسرعة. ويتطلب ذلك إعادة النظر في السياسات التنظيمية لتتماشى مع التطورات التقنية الحديثة وتوفير إطار قانوني يدعم ريادة الأعمال والابتكار.

5- الضغوط التنافسية: تواجه الشركات الناشئة منافسة شرسة من قبل الجهات الراسخة والمستثمرين الدوليين، مما يستدعي تبني استراتيجيات مبتكرة لتعزيز موقعها في السوق، تنعكس التحديات المالية والتنظيمية على قدرة الشركات على الابتكار وتطوير حلول جديدة تلبي احتياجات السوق المتغيرة. فالابتكار في مجال الأمن السيبراني يعتمد بشكل كبير على استثمارات ضخمة في البحث والتطوير، وفي غياب دعم كافٍ أو وجود أطر تنظيمية معيقة، قد يتراجع مستوى الابتكار مما يؤثر سلباً على القدرة التنافسية للشركات الناشئة.

6- الآثار الاجتماعية والاقتصادية: يُعتبر الأمن السيبراني عنصرًا أساسيًا لاستمرارية الأعمال وحماية المصالح الحيوية. لذا فإن ضعف استدامة شركات الأمن السيبراني قد يؤدي إلى زيادة المخاطر السيبرانية على المؤسسات الحيوية، مما ينعكس سلبًا على الاقتصاد الوطني ويزيد من تكاليف الأمان والحماية. (عزت، 2018، 35-36)

ج- الآثار والتبعات المترتبة على التحديات

إن الآثار على الأداء التشغيلي والمالي: إن الفجوات في تطبيق استراتيجيات الحوكمة والاستثمار في التقنيات الحديثة تؤدي إلى تراجع الأداء التشغيلي والمالي لشركات الأمن السيبراني الناشئة. فقد أظهرت الدراسات أن عدم مواكبة التغيرات التقنية وعدم توفر التمويل الكافي يؤدي إلى تأخر الشركات في طرح منتجاتها وخدماتها في السوق، مما يضعها في موقف تنافسي ضعيف أمام الشركات الكبرى.

د- أنواع الأمن السيبراني في الشركات الناشئة:

1- أمن البنية التحتية الحيوية: يعتمد على البنية التحتية الفيزيائية الإلكترونية للشبكة، وتتواجد عادة في وسائل النقل، والمدارس، والمستشفيات، والدوائر الحكومية، وفي شبكات المراكز التجارية. وهذا النوع يتطلب دراسة إلكترونية لنقاط ضعف المنظومة، والقاعدة الفيزيائية للشبكة لتطويرها وحمايتها من عمليات الاختراق.

2- تطبيقات الأمن السيبراني: وهو الاختيار السليم للبرامج التي تحمي الأجهزة والشبكات من عمليات الاختراق الإلكتروني، ولها عدة أنواع معروفة؛ أهمها: برامج مكافحة الفيروسات، والجدران النارية، وبرامج التشفير المعلوماتي. هذه الطرق الثلاثة تضمن لك حماية محتواك من عمليات الاختراق الإلكترونية؛ فكلما كان مستخدم الإنترنت أكثر اطلاعا على تكوين برامج الحماية ويستخدمها، كان أبعد عن احتمالية وقوعه رهن الابتزاز والاختراق.

3- أمن الشبكة: يهتم بالاختراقات الخارجية التي تهدد المنظومة الإلكترونية والمواقع التكنولوجية، فإن أمن الشبكة هو عملية تهتم بحماية الشبكة من الاختراقات الخارجية للشبكات والأجهزة. وهنالك عدة أنواع تضمن حصول أمن الشبكة؛ وهي: كلمات مرور جديدة، وبرامج الحماية من الفيروسات، وبرامج مكافحة التجسس، والجدران النارية.

4- سحابة الأمان: وهي نظام مراقبة وحماية لكل مصادر المعلومات والبي-انات التابعة للمستخدم عبر المواقع والمنصات الإلكترونية، ولكن إذا تم تفعيل هذه الخاصية لا يعني أنه بإمكانك تجاهل كل الأمور السيبرانية الأخرى، فمن الضروري الاهتمام بحماية المعلومات والبي-انات الخاصة بك بشكل مستمر.

5- إنترنت الأشياء: يشمل عدة منظومات أساسية، مثل: أجهزة التلفاز، وأجهزة الاستشعارات والطابعات، وهذا النوع صنف كنوع من الأمن السيبراني، الذي يحمي البيانات لدى الأجهزة المذكورة، ولكنه كباقي التقنيات؛ إذا لم يتم الاهتمام والمتابعة به يمكن أن يصل المخترق إلى نظام الحماية ويفك شفرته.

هـ- أبعاد دوافع اهتمام دولة السعودية بشركات الأمن السيبراني:

أولاً: البعد العسكري:

العديد من الدول بزيادة نفقاتها على بناء وتعزيز إمكانياتها السيبرانية. قد أصبح للفضاء السيبراني مكاناً مهمًا في استراتيجيات الأمن القومي، والاستراتيجيات العسكرية في العالم اليوم. ويرى العديد من الباحثين أن هذا ينذر ببدء ما يطلق عليه سباق التسلح الرقمي.

ثانياً: البعد السياسي:

تقوم القيادات السياسية العليا بتنظيم مؤسساتها المعلوماتية والأمنية وتقويتها، لكي تحمي مصالحها الوطنية والقومية، وكذلك تساعد باتخاذ القرارات المناسبة لإدارة الأزمات وحلها، أو إحباط الهجمات التي يشنها العدو لاستهداف المصالح القومية للدول.

ثالثاً: البعد الاجتماعي:

تؤدي الجريمة السيبرانية إلى العديد من الأضرار والآثار السلبية على المجتمع؛ حيث إنها تعتمد بصورة رئيسة على انتحال هوية الضحية في تعاملاته المالية والاجتماعية، وهذه الآثار لا تقتصر على الأفراد، ولكنها تمتد أيضًا إلى الشركات وبخاصة الشركات الناشئة، كما أن الحكومات من الأهداف الجذابة للأعمال الإجرامية السيبرانية، وهذه الجرائم تهدف بالأساس إلى إحداث العديد من الأضرار تجاه المجتمع ككل، وهذه الأضرار تستهدف تعطيل مصالح المواطنين في شبكات المواصلات والطاقة والشبكات المصرفية.

رابعاً: البعد الإعلامي:

تلعب وسائل الإعلام المختلفة دورًا كبيرًا في توعية أفراد المجتمع السعودي، باستخدام التقنية الحديثة للكشف عن الجرائم السيبرانية؛ لتوخي الحذر من الوقوع ضحية الهجمات السيبرانية المباشرة والموجهة، فيجب التعامل بحذر، بأخذ الحيطة والحذر، ورفع مستوى الأمان والتوعية، مثل: وضع كلمة مرور قوية، وتحديث الأجهزة وفق آخر ما وصلت إليه التقنية الحديثة، وتوجيه أبناء المجتمع نحو استخدام التقنية الحديثة استخدامًا سليمًا، من خلال عمل برامج تلفزيونية توعوية، وتوزيع نشرات توعوية عبر الصحف الورقية أو الإلكترونية، أو عبر وسائل التواصل الاجتماعي.

خامساً: البعد التعليمي:

يعتبر التركيز على إيجاد جيل متخصص في مجال الأمن السيبراني أمرًا مطلوبًا وحيويًا، وذلك للعمل كمتخصصين في هذا المجال الذي يعد من المجالات الحديثة والمهمة للتصدي للهجمات السيبرانية العابرة للقارات في هذا الفضاء السيبراني الكبير.

سادساً: البعد الاقتصادي:

تكمن أهميته في أن معظم الهجمات السيبرانية الخبيثة تستهدف المصالح الاقتصادية للأفراد والحكومات والقطاع الخاص؛ حيث يعتبر الاستغلال المالي هو الدافع الأول للجريمة السيبرانية التي تستهدف الأفراد والمؤسسات الحكومية وغير الحكومية؛ من أجل سرقة الأموال من حسابات الضحايا، وتحويلها إلى حسابات خارجية. ويقوم القراصنة باستخدام برامج تجسس، وهذه البرامج تساعد في الحصول على المعلومات السرية من الجهاز الخاص بالضحية، مثل: كلمات المرور في المواقع الإلكترونية المختلفة.

تاسعاً: الدراسات السابقة:

1- دراسة (Jayathilaka et al, 2024)

الهدف: تهدف هذه الدراسة إلى تطوير إطار عمل لتحديد الشركات الصغيرة والمتوسطة في سياق الأمن السيبراني، بالإضافة إلى تحسين نموذج ذكاء اصطناعي لتقديم توصيات أمنية مخصصة.

المنهج: استخدمت الدراسة منهجية PRISMA ومرت بأربع مراحل: التحديد، الفحص، الأهلية، والإدراج.

أداة الدراسة: واعتمدت على قواعد بيانات أكاديمية مثل Google Scholar، IEEE Xplore، وResearch Gate.

مجتمع وعينة الدراسة: المجتمع المستهدف هو الدراسات السابقة المتعلقة بالأمن السيبراني للشركات الصغيرة والمتوسطة، ولم يتم استخدام عينة بشرية مباشرة. بعد الفرز والتحليل، تم اختيار 43 دراسة عالية الجودة.

النتائج: أظهرت النتائج أن الحلول الأمنية المتخصصة غير مناسبة لمعظم SMEs بسبب ارتفاع التكلفة والتعقيد، كما أوضحت الدراسة وجود فجوة في تطبيق الذكاء الاصطناعي على مستوى هذه الشركات.

التوصيات: قدمت الدراسة إطارًا ونموذجًا أمنياً يعتمد على الذكاء الاصطناعي لتقديم حلول فعّالة، ميسورة، وقابلة للتطبيق.

2- دراسة (Zawaideh et al., 2023)

الهدف: هدفت الدراسة إلى تقييم مستوى استعداد الشركات الصغيرة والمتوسطة (SMEs) في مجال التجارة الإلكترونية لمواجهة التهديدات السيبرانية، وتحديد التهديدات الشائعة التي تواجهها في البيئة الرقمية. كما تسعى لاستكشاف كيفية استخدام تقنية البلوك تشين لتعزيز أمن العمليات الإلكترونية لهذه الشركات.

المنهج: اتبعت الدراسة منهجًا تطويريًا لبناء إطار العمل المقترح، اتبعت الدراسة منهجية متعددة الأساليب (mixed-methods)، حيث جمعت بين التحليلين النوعي والكمي.

أداة الدراسة: استخدمت التحليل النوعي: شمل إجراء مقابلات ومجموعات نقاش مركزة مع مالكي ومديري الشركات الصغيرة والمتوسطة وخبراء في الأمن السيبراني، لاستكشاف تجاربهم وتحدياتهم واستراتيجياتهم المتعلقة بالأمن السيبراني. والتحليل الكمي: تضمن إجراء مسح شامل لعينة ممثلة من هذه الشركات لجمع بيانات حول ممارساتها الأمنية، وتاريخ الحوادث الأمنية، وتصوراتها حول مخاطر الأمن السيبراني.

مجتمع وعينة الدراسة: استهدفت الدراسة الشركات الصغيرة والمتوسطة العاملة في مجال التجارة الإلكترونية.

النتائج: توصلت نتائجها إلى أن الشركات الصغيرة والمتوسطة تواجه مجموعة متزايدة من التهديدات السيبرانية التي قد تعرض بياناتها وسلامتها المالية وسمعتها للخطر. كما أوضحت أن تقنية البلوك تشين، بخصائصها مثل اللامركزية والشفافية وعدم القابلية للتغيير، يمكن أن تساعد في حماية البيانات الحساسة والتصدي للهجمات السيبرانية.

التوصيات: قدمت الدراسة توصيات عملية وقابلة للتطبيق لمساعدة الشركات الصغيرة والمتوسطة على تبني حلول أمن سيبراني فعالة ومناسبة لمواردها.

3- دراسة (Rodriguez-Baca et al., 2022)

الهدف: هدفت هذه الدراسة إلى فحص وتحليل حالة الأمن السيبراني في الشركات الصغيرة والمتوسطة في بيرو والمكسيك.

المنهج: استخدمت الدراسة منهج دراسة الحالة المتعددة.

أداة الدراسة: جمع البيانات النوعية والكمية عبر المسوح والمقابلات وتحليل الوثائق من عينة متنوعة من الشركات الصغيرة والمتوسطة في كلا البلدين.

مجتمع وعينة الدراسة:

النتائج: أسفرت النتائج عن تحديد التحديات والمخاطر السيبرانية الرئيسية التي تواجه هذه الشركات وتقييم ممارساتها الأمنية.

التوصيات: قدمت الدراسة توصيات عملية للشركات وصناع السياسات لتعزيز الأمن السيبراني في هذا القطاع الحيوي.

4- دراسة (المنيع، 2022):

الهدف: استهدفت التعرف على واقع تحقيق الأمن السيبراني في الجَامِعَات السعودية في ضوء رؤية 2030.

المنهج: استخدمت المنهج الوصفي التحليلي.

أداة الدراسة: اعتمدت الاستبانة.

مجتمع وعينة الدراسة: وتكون المجتمع البحثي للدراسة من جميع الموظفين التقنيين لثلاث جامعات سعودية هي: (جامعة أم القرى، جامعة الإمام عبدالرحمن بن فيصل، جامعة الإمام محمد بن سعود الإسلامية)، وقد اعتمدت الدراسة أسلوب العينة العشوائية، وقد بلغ العينة (210) موظفين

النتائج: توصلت إلى أن مفردات العينة موافقون بدرجة متوسطة على واقع تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية 2030، وأن مفردات العينة موافقون بدرجة كبيرة جدًّا على معوقات تحقيق الأمن السيبراني في الجَامِعات السعودية في ضوء رؤية 2030، ومن أهم هذه المعوقات تدني مستوى الخبرة لدى الموظفين، والضعف في التعاون بين موظفي التقنيات في الجامعات لتحقيق الأمن السيبراني. كما بينت النتائج وجود اتفاق بدرجة كبيرة جداً بين مفردات عينة الدراسة على متطلبات تحقيق الأمن السيبراني في الجَامِعَات السعودية في ضوء رؤية 2030.

التوصيات: كان من أهمها توعية العاملين بمخاطر استخدام الأجهزة الشخصية، المتمثلة في الهاتف المحمول لنقل أو تخزين معلومات سرية خاصة بالجامعة، ومنح الحوافز المادية والمعنوية المناسبة التي تعمل على دعم وتشجيع الموظفين المتميزين والمبدعين في مجال الأمن السيبراني.

5- دراسة (التيماني 2021):

الهدف: استهدفت هذه الدراسة معرفة واقع الأمن السيبراني لدي الأفراد في المجتمع السعودي كما يدركها الخبراء المتخصصين بأمن المعلومات.

المنهج: اعتمدت الدراسة على المنهج الوصفي.

أداة الدراسة: أداة المقابلة، والاستبانة الإلكترونية

مجتمع وعينة الدراسة: يتكون مجتمع الدراسة من جميع الأفراد العاملين في القطاع المصرفي والمختصين بإدارة أمن المعلومات، والأفراد العاملين بإدارة أمن المعلومات في القطاع التعليمي والمتمثل بالجامعات الحكومية في مدينة الرياض.

النتائج: توصلت النتائج هذه الدراسة إلي الاهتمام الحكومي بموضوع الأمن السيبراني بدأ بشكل مبكر قبل أن يدرك الأفراد في المجتمع هذا المفهوم، وأن أكثر أنماط الجرائم السيبرانية انتشارا بين الأفراد في المجتمع السعودي هي جريمة الاحتيال الإلكتروني، كما توصلت الدراسة إلى أن أكثر العوامل التي تزيد من فرصة حدوث الجرائم السيبرانية هو ضعف الوعي لدي الأفراد ومشاركتهم المعلومات الشخصية مع الآخرين دون دراية ومعرفة بطبيعة عمل هؤلاء الأشخاص.

6- دراسة (البغدادي 2021)

الهدف: هدفت الدراسة إلى تسليط الضوء على التحديات التي يواجهها المجتمع المصري في تحقيق الأمن السيبراني.

المنهج: تم استخدام المنهج التحليلي والمقارن.

أداة الدراسة: الاستبانة الرقمية.

مجتمع وعينة الدراسة:

النتائج: أوضحت الدراسة أن التحول الرقمي في مصر أدى إلى زيادة استخدام الإنترنت والتكنولوجيا والمعاملات الإلكترونية، وزادت في المقابل حالات الهجمات السيبرانية.

التوصيات: دعت الباحثة إلى ضرورة الاستفادة من التجارب الحديثة وإلى إنشاء إطار تعاوني بين الدول العربية في مجال الأمن السيبراني.

7- دراسة (السمحان، 2020)

الهدف: أجرت هذه الدراسة تحليلاً لكيفية تحقيق الأمن السيبراني في جامعة الملك سعود من خلال تقييم المتطلبات الإدارية التقنية البشرية، والمادية.

المنهج:

أداة الدراسة: تم استخدام استبانة كأداة لجمع المعلومات

مجتمع وعينة الدراسة: عينة تضم 384 من موظفي الجامعة

النتائج: أظهرت النتائج أن الجامعة تمتلك وسائل مهمة تعزز حماية أنظمة المعلومات الإدارية في الجامعة.

التوصيات:

التعقيب على الدراسات السابقة

يتضح من خلال استعراض الدراسات السابقة تنوع الجهود البحثية التي سعت إلى استكشاف واقع الأمن السيبراني من زوايا متعددة، سواء على مستوى الشركات الصغيرة والمتوسطة أو المؤسسات التعليمية، وكذلك من خلال تحليل التوجهات الفردية والمجتمعية تجاه هذه القضية. وقد أظهرت تلك الدراسات نقاط التقاء مهمة مع موضوع الدراسة الحالية، وفي ذات الوقت كشفت عن عدد من الفجوات التي تبرر أهمية تناول "واقع استدامة شركات الأمن السيبراني الناشئة في ضوء توجهات الأفراد في المجتمع السعودي" كمجال بحثي مستقل.

فقد تناولت دراسة (Jayathilaka et al., 2024) تحديات تبني الذكاء الاصطناعي في شركات الSMEs، ووضّحت ضعف ملاءمة الحلول التقنية التقليدية لهذه الشركات، مما يسلط الضوء على حاجة ملحة لحلول أمنية مرنة ومستدامة. وهذا يتقاطع مع الدراسة الحالية من حيث تأكيد الحاجة إلى نماذج عمل قابلة للتطبيق في بيئات ناشئة تعتمد على الابتكار والذكاء الاصطناعي.

أما دراسة (Zawaideh et al., 2023) فقد ركّزت على قابلية الشركات الصغيرة والمتوسطة لمواجهة التهديدات السيبرانية، واقترحت البلوك تشين كحل مبتكر، مما يدعم أهمية توظيف تقنيات حديثة ومستدامة وهو ما يتوافق مع فرضيات الدراسة الحالية التي تفترض أن التوجهات الفردية نحو الابتكار تؤثر على استدامة شركات الأمن السيبراني الناشئة.

في حين قدّمت دراسة (Rodriguez-Baca et al., 2022) رؤية واقعية للتحديات الأمنية في دول أمريكا اللاتينية، مما يعزز إمكانية المقارنة مع السياق السعودي ويمنح الدراسة الحالية بعدًا مقارنًا فيما يتعلق بفعالية الممارسات الأمنية الإقليمية والدولية ومدى قابليتها للتوطين في السوق السعودي.

أما الدراسات المحلية مثل دراسة (المنيع، 2022) ودراسة (السمحان، 2020)، فقد ركّزت على واقع الأمن السيبراني في الجامعات السعودية، وقدّمت تصورًا دقيقًا حول التحديات الإدارية والبشرية، مما يساعد على فهم البيئة المؤسسية السعودية بشكل عام، ويمكن أن يُستفاد من نتائجها في دراسة استعداد الأفراد والمؤسسات الناشئة لتبني ثقافة الأمن السيبراني وتعزيز استدامتها.

كذلك فإن دراسة (التيماني، 2021) تبرز البعد الفردي في تعامل الأفراد مع الأمن السيبراني، من حيث الوعي والممارسات، وهي نقطة محورية في الدراسة الحالية التي تسعى إلى فهم كيف تؤثر التوجهات الفردية في دعم أو إضعاف استدامة الشركات السيبرانية.

أما دراسة (البغدادي، 2021) فقد سلطت الضوء على الواقع المصري، وناقشت الأثر المجتمعي والتحول الرقمي على مستوى الأمن السيبراني، ما يُعد مرجعًا مفيدًا في ضوء أوجه التشابه الثقافي والاجتماعي بين المجتمعين المصري والسعودي، مما يعزز القدرة على استقراء فرص وتحديات استدامة شركات الأمن السيبراني.

من خلال ما سبق، يتضح أن أغلب الدراسات ركزت على الأمن السيبراني من منظور التهديدات، الجاهزية المؤسسية، أو القدرات التقنية، لكنها لم تتناول بشكل مباشر استدامة الشركات السيبرانية الناشئة في ضوء التوجهات الفردية، لا سيما في السياق السعودي. وهنا تكمن مساهمة الدراسة الحالية في سد هذه الفجوة البحثية، من خلال دمج البعدين المجتمعي والاقتصادي في دراسة استدامة قطاع يُعد من أكثر القطاعات حيوية في ظل التحول الرقمي ورؤية السعودية 2030.

عاشراً: منهجية الدراسة وإجراءاتها:

1- منهج الدراسة:

اتبع الباحث المنهج الوصفي التحليلي، كونه الأنسب لطبيعة أهداف البحث التي تسعى إلى وصف واقع استدامة شركات الأمن السيبراني الناشئة في المملكة العربية السعودية، وتحليل مدى وعي وثقة الأفراد في المجتمع تجاه الخدمات التي تقدمها هذه الشركات. كما يتيح هذا المنهج فحص العلاقات والاتجاهات القائمة بين المتغيرات المدروسة، واستقراء النتائج بناءً على البيانات الفعلية الميدانية.

2- مجتمع وعينة البحث:

أ- مجتمع الدراسة:

يتكون مجتمع الدراسة من العاملين في شركات الأمن السيبراني الناشئة في المملكة العربية السعودية من الجنسين، ممن يشغلون وظائف إدارية وفنية، إضافة إلى عدد من الأفراد من المجتمع السعودي المستفيدين من خدمات هذه الشركات: (شركة Cipher، شركة CQR، شركة COGNNA) (والتي تمارس أنشطتها في مجالات حماية البيانات، واختبار الاختراق، وتطوير حلول أمنية رقمية)، لقياس وعيهم وتوجهاتهم نحو أهمية هذه الخدمات ومدى ثقتهم في استدامتها.

ب- عينة الدراسة:

تكونت العينة من فئتين رئيسيتين:

العينة الأولى: تضم العاملين في شركات Cipher، وCQR، وCOGNNA من متخذي القرار في المستويات الإدارية العليا والوسطى والوظائف التقنية، وعددهم (170) فردًا.

العينة الثانية: فتضم (80) فردًا من مستخدمي خدمات هذه الشركات داخل المجتمع السعودي.

وقد لبلغ حجم العينة الإجمالي (250). وبعد جمع الاستجابات عبر استبانة إلكترونية، تم استبعاد الردود غير المكتملة، ليبلغ عدد الاستبانات الصالحة للتحليل الإحصائي (150 استبانة).

خصائص أفراد الدراسة وتحليلها:

أ- فئة المشاركة في الدراسة

جدول (1): توزيع أفراد عينة الدراسة

العينة	التكرار	النسبة (%)
العاملون في شركات الأمن السيبراني الناشئة	**84**	**56.0**

العينة	التكرار	النسبة (%)
مستخدمو خدمات هذه الشركات من المجتمع السعودي	**66**	**44.0**
المجموع	**150**	**100%**

يوضح الجدول (1) توزيع أفراد الدراسة وفقًا للعينة، حيث بلغت نسبة العاملين في شركات الأمن السيبراني الناشئة (Cipher، CQR، COGNNA) نحو 56.0% من إجمالي العينة، وهم من متخذي القرار في الإدارات العليا والوسطى إضافة إلى الموظفين في الأقسام التقنية. بينما بلغت نسبة مستخدمي خدمات هذه الشركات من الأفراد داخل المجتمع السعودي نحو 44.0%، وهو ما يعكس اهتمام الدراسة بقياس واقع الاستدامة من زاويتين: داخلية تمثّل العاملين، وخارجية تمثّل المستفيدين من الخدمات.

ب- الجنس:

جدول (2): توزيع أفراد عينة الدراسة وفقًا لمتغير الجنس

العينة	التكرار	النسبة (%)
ذكور	**105**	**70.0%**
إناث	**45**	**30.0%**
المجموع	**150**	**100%**

يوضح الجدول (2) توزيع خصائص عينة الدراسة وفقاً لمتغير الجنس، وقد تبين نسبة الذكور70.0% من إجمالي العينة، وهي الفئة الأكبر من بين فئات الدراسة، في حين أن تشكل نسبة الإناث 30.0% من إجمالي أفراد الدراسة، وهي الفئة الأقل من بين فئات الدراسة.

ج- سنوات الخبرة العملية

جدول (3): توزيع أفراد عينة الدراسة وفقًا لمتغير سنوات الخبرة العملية

العينة	التكرار	النسبة (%)
أقل من 5 سنوات	**75**	**50.0%**
من 5 إلى 10 سنوات	**45**	**30.0%**
أكثر من 10 سنوات	**30**	**20.0%**
المجموع	**150**	**100%**

يوضح الجدول (3) توزيع أفراد عينة الدراسة وفقًا لمتغير **سنوات الخبرة العملية**. يبين الجدول أن**50.0%** من أفراد العينة لديهم **أقل من 5 سنوات** من الخبرة العملية، مما يعكس الطبيعة الناشئة لشركات الأمن السيبراني في المملكة العربية السعودية، حيث أن العديد من هذه الشركات تعتبر حديثة العهد في السوق، أما**30.0%** من الأفراد في العينة لديهم **من 5 إلى 10 سنوات** من الخبرة العملية، وهذه الفئة تعكس الخبرة المتوسطة التي تكتسبها شركات الأمن السيبراني الناشئة في مرحلة التوسع والابتكار، وأخيرًا،**20.0%** من الأفراد لديهم **أكثر من 10 سنوات** من الخبرة، ويعود ذلك إلى وجود بعض الأفراد الذين انتقلوا للعمل في شركات الأمن السيبراني من شركات أخرى قديمة ذات خبرة طويلة في المجال التقني.

د- المؤهل العلمي:

جدول (4): توزيع أفراد الدراسة وفقًا لمتغير المؤهل العلمي

العينة	التكرار	النسبة (%)
دبلوم	**2**	**1.3%**
بكالوريوس	**108**	**72.0%**
ماجستير	**36**	**24.0%**
دكتوراه	**4**	**2.7%**
المجموع	**150**	**100%**

يوضح الجدول (4) خصائص عينة أفراد الدراسة من رؤساء الإدارات، ومديري الأقسام، والتقنيين، ومستخدمي خدمات الشريكات بالمملكة العربية السعودية وفقاً لمتغير المؤهل العلمي، وقد تبين أن ما نسبته (**72.0%**) من إجمالي أفراد الدراسة مؤهلهم العلمي بكالوريوس، وهي الفئة الأكبر من بين فئات الدراسة، في حين وجد أن ما نسبته (**24.0%**) من إجمالي أفراد الدراسة ماجستير، في حين وجد أن ما نسبته (**2.7%**) من إجمالي أفراد الدراسة دكتوراه، في حين وجد أن ما نسبته (**1.3%**) من إجمالي أفراد الدراسة مؤهلهم العلمي دبلوم، وهي الفئة الأقل من بين فئات الدراسة

3- أداة الدراسة:

لتحقيق هدف الدراسة، اعتمد الباحث على الأدوات التالية للحصول على البيانات والمعلومات:

1- المصادر الثانوية: المعلومات المتعلقة بالجانب النظرية. وقد شملت البحوث والدراسات السابقة، والمقالات، والرسائل الجامعية، والكتب العلمية المتخصصة التي تناولت موضوعات الأمن السيبراني، استدامة الشركات الناشئة، وأمن المعلومات المتعلقة بموضوع الدراسة.

2- المصادر الأولية (الاستبانة): لتوفير البيانات المتعلقة بجوانب الدراسة، تم تصميم الاستبانة كأداة أساسية لجمع البيانات. وقد تم تصميم الاستبانة بعد أخذ آراء مجموعة من الباحثين والمتخصصين في مجال الأمن السيبراني لتتناسب مع أهداف الدراسة بشكل دقيق. وقد تم اعتبار الاستبانة الأداة المنظمة والضابطة لجميع بيانات الدراسة من خلال نموذج الأسئلة الموجهة إلى كل من التقنيين والإداريين العاملين في الشركات الناشئة للأمن السيبراني مثل شركة Cipher، شركة CQR، وشركة COGNNA، بهدف الحصول على بيانات دقيقة حول التوجهات نحو استدامة هذه الشركات.

وتضم الاستبانة قسمين رئيسيين هما: القسم الأول: من الاستبانة يحتوي على البيانات الديموغرافية للأفراد المشاركين في الدراسة، ويتضمن الجنس، سنوات الخبرة، والمؤهل العلمي. **والقسم الثاني:** من الاستبانة يشتمل على محاور الدراسة المرتبطة بالاستدامة في شركات الأمن السيبراني، وتشمل أسئلة حول مدى تأثير الابتكار التكنولوجي، التوجهات المجتمعية، الوعي بالأمن السيبراني، ومدى الاستدامة التنظيمية في هذه الشركات. وتم استخدام **مقياس ليكرت الخماسي** في صياغة الأسئلة (لا أوافق بشدة، لا أوافق، محايد، أوافق، أوافق بشدة). وتحتوي الاستبانة على 13 عبارة.

صدق أداة الدراسة:

تمّ التحقق من صدق الاستبانة على طريقتين:

أ- الصدق الظاهري:

يهتم هذا الجانب بالصورة الخارجية لأداة الدراسة من حيث بنية العبارات وموضعيتها وأهميتها، كذلك التراكيب اللغوية ومدى مناسبتها بالنسبة للأفراد المستهدفين بالدراسة، كما يهتم هذا الجانب بمدى ملائمة أداة الدراسة للهدف الذي وضعت من أجله، ومدى اتساقها مع تساؤلات الدراسة. ولقياس هذا الصدق تمّ عرض الاستبانة بصورتها الأولية على لجنة التحكيم؛ وذلك لاستطلاع آرائهم حول ملاءمة وارتباط عبارات الأداة مع المحاور التي تقيسها، إضافة لإبداء رأيهم حول صحة وسلامة الصياغة اللغوية، وبعد إجراء التعديلات حسب ملاحظات المحكمين، تمّ اعتماد العبارات والمحاور التي اتفق عليها أغلب المحكمين، حتى أخذت الاستبانة شكلها النهائي.

ب- صدق الاتساق الداخلي:

بعد التأكد من الصدق الظاهري لأداة الدراسة قام الباحث بتطبيقها على مجتمع الدراسة؛ وذلك من خلال الاتساق الداخلي، ومعرفة مدى اتساق كل عبارة من عبارات الأداة مع المحور الذي تنتمي إليه هذه العبارة. ولحساب صدق الاتساق الداخلي للأداة تمّ حساب معامل ارتباط بيرسون (Pearson Correlation Coefficient) والذي من خلاله تمّ حساب معاملات الارتباط بين درجة كل عبارة والدرجة الكلية للمحور الذي تنتمي إليه؛ وذلك بهدف التحقق من مدى صدق الأداة ككل، وذلك عبر عينة استطلاعية من خارج عينة الدراسة.

وفيما يأتي عرض لنتائج صدق الاتساق الداخلي:

1- تم حساب معاملات الارتباط لكل عبارة في هذا المحور مع الدرجة الكلية للمحور، ووجد أن جميع القيم كانت إيجابية وعالية بما يتناسب مع المعايير الأكاديمية المتعارف عليها. مما يدل على أن العبارات في هذا المحور تتسق بشكل جيد مع الهدف المخصص لها، وبالتالي تعكس بشكل دقيق وموثوق واقع استخدام الأمن السيبراني في الشركات الناشئة في المملكة.

جدول (5): معاملات الارتباط بين درجة كل عبارة من عبارات محور "و اقع استخدام تقنية الأمن السيبر اني في الشركات الناشئة بالمملكة العربية السعودية" بالدرجة الكلية للمحور

رقم العبارة	معامل الارتباط بالمحور	رقم العبارة	معامل الارتباط بالمحور
1	**0.586	9	**0.571
2	**0.639	10	**0.702
3	**0.577	11	**0.641
4	**0.712	12	**0.614
5	**0.727	13	**0.723
6	**0.808	14	**0.711

رقم العبارة	معامل الارتباط بالمحور	رقم العبارة	معامل الارتباط بالمحور
7	**0.746	15	**0.636
8	**0.638	16	**0.716

** دالة عند مستوى الدلالة 0.01 فأقل.

يتضح من الجدول السابق رقم (5) أن قيم معامل ارتباط كل عبارة من العبارات مع الدرجة الكلية لمحور "واقع استخدام تقنية الأمن السيبراني في الشركات الناشئة بالمملكة العربية السعودية" الذي تنتمي إليه العبارة موجبة ودالة إحصائياً عند مستوى الدلالة (0.01) فأقل، وذات قيم مرتفعة؛ مما يشير إلى أن عبارات هذا المحور تتمتع بدرجة صدق مرتفعة وصلاحيتها للتطبيق الميداني.

2- صدق الاتساق الداخلي لمحور "التوجهات والخطط المستقبلية لتقنية الأمن السيبراني في الشركات الناشئة بالمملكة العربية السعودية"

جدول (6): معاملات الارتباط بين درجة كل عبارة من عبارات محور"التوجّهات والخطط المستقبلية لتقنية الأمن السيبر اني في الشركات الناشئة بالمملكة العربية السعودية" بالدرجة الكلية للمحور

رقم العبارة	معامل الارتباط بالمحور	رقم العبارة	معامل الارتباط بالمحور
1	**0.882	8	**0.866
2	**0.886	9	**0.776
3	**0.816	10	**0.869
4	**0.735	11	**0.868
5	**0.677	12	**0.873
6	**0.866	13	**0.839
7	**0.891		

ملاحظة: جميع القيم دالة عند مستوى الدلالة (0.01) فأقل.

يتضح من الجدول (7) أن قيم معامل ارتباط كل عبارة من العبارات مع الدرجة الكلية لمحور "التوجّهات والخطط المستقبلية لتقنية الأمن السيبراني في الشركات الناشئة بالمملكة العربية السعودية" جاءت جميعها موجبة وذات دلالة إحصائية عند مستوى (0.01) فأقل، وذات قيم مرتفعة؛ مما يشير إلى أن عبارات هذا المحور تتمتع بدرجة صدق مرتفعة وصلاحيتها للتطبيق الميداني.

ثبات أداة الدراسة:

المقصود بثبات الاستبانة هو أن تعطي النتائج نفسها تقريبًا لو تم تكرار تطبيقها أكثر من مرة على نفس الأفراد في ظروف مماثلة. وسيتم حساب ثبات أداة الدراسة (الاستبانة) باستخدام **معامل ألفا كرونباخ(Cronbach's Alpha)**، اشتق كرونباخ عام 1951 هذه المعادلة من معادلة كيودر ريتشاردسون 20 (KR-20)، وتم تطويرها لاحقًا على يد "كايز وميشل" عام 1975م تحت مسمى "معامل ألفا"Coefficient، وفيها يحل مجموع تباينات درجات جميع الأسئلة محل مجموع حاصل ضرب نسبة الأفراد الذين أجابوا إجابة صحيحة على كل سؤال، ونسبة الذين لم يجيبوا على السؤال. والجدول رقم (7) يوضح معامل الثبات لمحاور أداة الدراسة وهي:

جدول (7) معامل ألفا كرونباخ لقياس ثبات أداة الدراسة

المحاور	عدد العبارات	معامل الثبات
و اقع استخدام تقنية الأمن السيبر اني في الشركات الناشئة بالمملكة العربية السعودية	16	0.915
التوجهات والخطط المستقبلية لتقنية الأمن السيبر اني في الشركات الناشئة بالمملكة العربية السعودية	13	0.961
الثبات الكلي للاستبانة	29	0.94

يتضح من النتائج الموضحة في جدول (8) أن معاملات الثبات لمحوري الاستبانة تتراوح ما بين (0.915-0.961)، بينما بلغت قيمة معامل الثبات العام (0.94)، وهي قيمة مرتفعة تشير إلى أن أداة الدراسة تتمتع بدرجة عالية من الثبات، مما يؤكد صلاحيتها للتطبيق الميداني.

الأساليب الإحصائية لتحليل بيانات الاستبانة:

لتحقيق أهداف الدراسة وتحليل البيانات التي تم جمعها، تم استخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية SPSS، وذلك بعد ترميز وإدخال البيانات إلى الحاسب الآلي، حيث أعطيت الإجابة: أوافق بشدة (5) درجات، موافق (4) درجات، محايد (3) درجات، لا أوافق (2) درجتان، لا أوافق بشدة (1) درجة واحدة. ومن ثم قام الباحث بحساب الوسط الحسابي لإجابات أفراد الدراسة.

ولتحديد طول خلايا المقياس الخماسي (الحدود الدنيا والعليا) المستخدم في محاور الدراسة، تم حساب المدى (5-1 =4)، ثم تقسيمه على عدد خلايا المقياس للحصول على طول الخلية الصحيح أي (5/4 =0.80) بعد ذلك تم إضافة هذه القيمة إلى أقل قيمة في المقياس؛ وذلك لتحديد الحد الأعلى لهذه الخلية.

أساليب المعالجة الإحصائية:

لخدمة أغراض الدراسة وتحليل البيانات التي تم تجميعها، استخدم الباحث الأساليب الإحصائية الآتية:

1- التكرارات والنسب المئوية للتعرف على الخصائص الشخصية والوظيفية لعينة الدراسة، وتحديد استجابات أفرادها تجاه عبارات المحاور الرئيسية التي تتضمنها الدراسة.

2- المتوسط الحسابي، والانحراف المعياري لمعرفة مدى استجابات أفراد عينة الدراسة عن كل محور من المحاور وكل عبارة من عبارات المحور.

3- معامل ارتباط بيرسون للتأكد من صدق الاتساق الدّاخلي؛ وذلك من خلال معرفة درجة الارتباط بين عبارات الاستبانة، والمحور الذي تنتمي إليه كل عبارة من عبارته.

4- معامل ألفا كرونباخ لحساب معامل ثبات المحاور المختلفة لأداة الدراسة.

حادي عشر: النتائج الخاصة باختبار فروض الدراسة:

عرض وتفسير الجداول الخاصة بالفرض الثاني: "توجد علاقة ذات دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين مدى تطبيق معايير الأمن السيبراني، وبين الفاعلية التنظيمية لشركات الأمن السيبراني الناشئة. **استخدم الباحث** المتوسطات الحسابية والانحرافات المعيارية كما قام بترتيب العبارات تنازليا، وعلى النحو الوارد في الجدول الآتي:

جدول رقم (8): المتوسطات الحسابية والانحرافات المعيارية لإجابات عينة الدراسة على عبارات بين مدى تطبيق معايير الأمن السيبراني، وبين الفاعلية التنظيمية لشركات الأمن السيبراني الناشئة بالمملكة العربية السعودية مرتبة تنازليا حسب المتوسطات

م	العبارة	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الموافقة
1	تحرص الشركة التي أعمل بها على تطبيق أحدث أدوات وتقنيات الأمن السيبراني في عملياتها التشغيلية.	4.80	0.40	1	أوافق بشدة
8	تعتمد الشركة بشكل أساسي على حماية البنية التحتية الرقمية لديها باستخدام معايير أمنية متقدمة.	4.79	0.47	2	
2	توفر الشركة تدريبًا مستمرًا للموظفين لتعزيز وعيهم بممارسات الأمن السيبراني.	4.75	0.52	3	
11	تلتزم الشركة بالمعايير العالمية المعتمدة لأمن المعلومات مثل ISO 27001.	4.72	0.63	4	أوافق بشدة
7	لدى الشركة سياسات واضحة ومعلنة للاستجابة للحوادث الأمنية والاختراقات.	4.71	0.61	5	
12	تستخدم الشركة تقنيات الحماية السحابية لتأمين بيانات العملاء والخوادم.	4.71	0.56	6	
3	تعتمد الشركة على حلول أمنية متقدمة لحماية الشبكات من الهجمات السيبرانية.	4.69	0.57	7	أوافق بشدة
9	توجد خطة استمرارية عمل واستعادة بيانات في حال وقوع أي هجمات إلكترونية.	4.61	0.65	8	
10	يتم تحديث البرمجيات الأمنية المستخدمة بشكل دوري في الشركة.	4.61	0.67	9	
5	تشجع الإدارة استخدام الابتكار والتقنيات الحديثة في مجال الأمن السيبراني.	4.57	0.66	10	أوافق بشدة

م	العبارة	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الموافقة
4	تضع الإدارة العليا خططا تتسم بالمرونة الكافية لاستيعاب أي تغيرات ومستجدات يتطلبها تبني تقنية الإجراءات الوقائية.	4.56	0.64	11	
6	توفر الشركة نظام رقابة داخلي لرصد أي نشاط غير معتاد في الأنظمة الرقمية.	4.48	0.70	12	أو افق بشدة
13	يتم إشراك الموظفين في صياغة سياسات الأمن السيبر اني لتحقيق الالتزام المؤسسي.	4.41	0.82	13	
	المتوسط الحسابي العام	4.65	0.61	أو افق بشدة	

يتضح من الجدول السابق ما يأتي:

يتضح من الجدول السابق وجود تقارب في درجة موافقة أفراد العينة من موظفي الشركات الناشئة في قطاع الأمن السيبراني (مثل Cipher، CQR، وCOGNNA) على العبارات المرتبطة بتطبيق أدوات وتقنيات الأمن السيبراني؛ حيث يشمل المحور (13) عبارة، إذ تراوحت المتوسطات الحسابية بين (4.41 إلى 4.80)، وهي جميعها تقع ضمن الفئتين الرابعة والخامسة من مقياس ليكرت الخماسي، أي بدرجة (موافق) و(موافق بشدة) بالنسبة لأداة الدراسة.

كشفت متوسطات المحور عن مستويات إجابات أفراد عينة الدراسة، وقد كانت أعلى عبارة من حيث المتوسط الحسابي هي **العبارة رقم (1)** والتي نصها "تحرص الشركة التي أعمل بها على تطبيق أحدث أدوات وتقنيات الأمن السيبراني في عملياتها التشغيلية." **بالمرتبة الأولى** وبدرجة (موافق بشدة)، بمتوسط حسابي (4.80) وانحراف معياري (0.40)؛ وتفسير ذلك على وعي الشركات الناشئة وأفراد المجتمع المستفيدين منها بأهمية دمج أحدث التقنيات لضمان حماية أنظمتها التشغيلية والبيانات الحساسة من المخاطر السيبرانية.

يليها **العبارة رقم (8)** والتي نصها "تعتمد الشركة بشكل أساسي على حماية البنية التحتية الرقمية لديها باستخدام معايير أمنية متقدمة". **بالمرتبة الثانية** وبدرجة (موافق بشدة)، بمتوسط حسابي (4.79) وانحراف معياري (0.47)؛ وتفسير ذلك أنه يؤكد أن البنية التحتية الآمنة تعد حجر الزاوية في عمل هذه الشركات.

ثم جاءت **العبارة رقم (2)** والتي نصها "توفر الشركة تدريبًا مستمرًا للموظفين لتعزيز وعيهم بممارسات الأمن السيبراني" **بالمرتبة الثالثة** وبدرجة (موافق بشدة)، بمتوسط حسابي (4.75) وانحراف معياري (0.52) ويعكس هذا التزام الشركات بتطوير القدرات البشرية كجزء أساسي من استراتيجيات الحماية.

وفي سياق متصل جاءت **العبارة رقم (11)** والتي نصها ""تلتزم الشركة بالمعايير العالمية المعتمدة لأمن المعلومات مثل ISO 27001" **بالمرتبة الرابعة** وبدرجة (موافق بشدة)، بمتوسط حسابي (4.72) وانحراف معياري (0.63)؛ وتفسير ذلك أن مؤشر على أن هذه الشركات تراعي الامتثال للممارسات والمعايير الدولية، مما يعزز موثوقيتها في السوق.

بينما تلتها **العبارة رقم (7)** والتي نصها "لدى الشركة سياسات واضحة ومعلنة للاستجابة للحوادث الأمنية والاختراقات" **بالمرتبة الخامسة** وبدرجة موافقة (موافق بشدة)، بمتوسط حسابي (4.71) وانحراف معياري (0.61)؛ وتفسير ذلك إلى وجود إطار مؤسسي للاستجابة السريعة للمخاطر المحتملة.

كما جاءت **العبارة رقم (12)** والتي نصها "تستخدم الشركة تقنيات الحماية السحابية لتأمين بيانات العملاء والخوادم"، **بالمرتبة السادسة** وبدرجة (موافق بشدة)، بمتوسط حسابي (4.71) وانحراف معيا(0.56) ؛ ويفسر هذا التوجه المتزايد نحو استخدام الخدمات السحابية كخيار ذكي وآمن لتخزين البيانات.

وفي سياق متصل جاءت **العبارة رقم (3)** والتي نصها "تعتمد الشركة على حلول أمنية متقدمة لحماية الشبكات من الهجمات السيبرانية"، **بالمرتبة السابعة** وبدرجة موافقة (موافق بشدة)، بمتوسط حسابي (4.69) وانحراف معياري(0.56) ؛ وهذا يتفق مع الحاجة المستمرة لتعزيز الدفاعات ضد التهديدات الشبكية المتزايدة.

بينما تلها **العبارة رقم (9)** والتي نصها "توجد خطة استمرارية عمل واستعادة بيانات في حال وقوع أي هجمات إلكترونية", **بالمرتبة الثامنة** جاءت بمتوسط (4.61) وانحراف (0.65)، ودرجة (أوافق بشدة)، ما يدل على وجود استعداد جيد لمواجهة الأزمات وضمان استمرارية العمليات.

بينما تلتها **العبارة رقم (10)** والتي نصها "يتم تحديث البرمجيات الأمنية المستخدمة بشكل دوري في الشركة"، **بالمرتبة التاسعة** وبدرجة (موافق بشدة)، بمتوسط حسابي (4.57) وانحراف معياري (0.66)؛ ما يبرز أهمية الصيانة الدورية كنقطة محورية في حماية الأنظمة.

كما جاءت **العبارة رقم (5)** والتي نصها " "تشجع الإدارة استخدام الابتكار والتقنيات الحديثة في مجال الأمن السيبراني"، **بالمرتبة العاشرة** وبدرجة (موافق بشدة)، بمتوسط حسابي (4.57) وانحراف معياري (0.66). ما يعكس مرونة الإدارة في التجاوب مع التطورات التقنية المستجدة.

ثم جاءت **العبارة رقم (4)** والتي نصها "تضع الإدارة العليا خطط تتسم بالمرونة الكافية لاستيعاب أي تغيرات ومستجدات يتطلبها تبني تقنية الحوسبة السحابية" **بالمرتبة الحادية عشر** وبدرجة (موافق بشدة)، بمتوسط حسابي (4.56) وانحراف معياري (0.64)؛ ما يشير إلى تبني استراتيجيات تخطيط ديناميكية تأخذ في الاعتبار تغيرات البيئة التقنية.

وفي سياق متصل جاءت العبارة رقم (6) والتي نصها "توفر الشركة نظام رقابة داخلي لرصد أي نشاط غير معتاد في الأنظمة الرقمية"، **بالمرتبة الثاني عشر** وبدرجة (موافق بشدة)، بمتوسط حسابي (4.29) وانحراف معياري (0.86)، مما يدل على الاهتمام بالرصد الاستباقي للتهديدات الداخلية.

كما جاءت العبارة رقم (13) والتي نصها يتم إشراك الموظفين في صياغة سياسات الأمن السيبراني لتحقيق الالتزام المؤسسي". **بالمرتبة الثالث عشر** وبدرجة (موافق بشدة)، بمتوسط حسابي (4.61) وانحراف معياري (0.67). ويعكس هذا توجّهًا نحو الشفافية والشمولية في صناعة القرار الأمني.

نستخلص ممّا سبق أن المتوسط العام لاستجابات أفراد الدراسة على عبارات محور **(و اقع استخدام تقنيات الأمن السيبر اني في الشركات الناشئة بالمملكة العربية السعودية)** قد بلغ **(4.65 درجة من 5)**، وهذا المتوسط يقع في **الفئة الخامسة من فئات المقياس الخماسي** التي تشير إلى درجة **(مو افق بشدة)** بالنسبة لأداة الدراسة. وقد أظهر أفراد الدراسة موافقتهم الشديدة على أن واقع استخدام تقنيات الأمن السيبراني في الشركات الناشئة يتجلى من خلال العوامل التالية:

1- تقوم الشركة باستخدام تقنيات الأمن السيبراني لحماية أنظمتها الرقمية من أي هجمات أو اختراقات.
2- تقوم الشركة بتحديث أدوات الحماية بشكل دوري لمواكبة التغيرات الأمنية المتسارعة.
3- تسعى الشركة لتدريب موظفيها على سبل الأمن السيبراني والتوعية الرقمية.
4- تعتمد الشركة سياسات واضحة للتحكم في الصلاحيات والوصول إلى البيانات الحساسة.
5- تستخدم الشركة أدوات متقدمة لرصد التهديدات الأمنية والاستجابة لها.
6- تعمل الشركة على إجراء اختبارات دورية لتقييم قوة أنظمتها الدفاعية وكشف الثغرات.

عرض وتفسير الجداول الخاصة بالفرض الثالث: توجد علاقة ذات دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين التزام شركات الأمن السيبراني الناشئة بتطبيق معايير الأمن السيبراني وتحسين الكفاءة التشغيلية

جدول رقم (11): المتوسطات الحسابية والانحر افات المعيارية لإجابات عينة الدراسة على عبارات التزام شركات الأمن السيبر اني الناشئة بتطبيق معايير الأمن السيبر اني وتحسين الكفاءة التشغيلية، مرتبة تنازليًا بحسب المتوسطات

م	العبارة	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة المو افقة
2	التزام شركات الأمن السيبر اني الناشئة بتطبيق معايير الأمن السيبر اني يعزز من قدرة الشركة على تحسين كفاءتها التشغيلية.	4.67	0.50	1	أو افق بشدة
1	الشركات التي تلتزم بمعايير الأمن السيبر اني تتمتع بقدرة أعلى على مواجهة التهديدات الإلكترونية، مما يزيد من كفاءتها التشغيلية.	4.63	0.59	2	أو افق بشدة
11	الدعم الحكومي لمعايير الأمن السيبر اني يسهم بشكل كبير في تحسين الكفاءة التشغيلية لشركات الأمن السيبر اني الناشئة.	4.61	0.54	3	أو افق بشدة
3	تطبيق معايير الأمن السيبر اني يوفر بيئة آمنة للبيانات، مما يعزز من كفاءة العمليات التشغيلية.	4.60	0.57	4	أو افق بشدة
12	الشركات الناشئة التي تلتزم بمعايير الأمن السيبر اني تكون أكثر قدرة على توفير خدمات موثوقة، مما يسهم في تحسين الكفاءة التشغيلية.	4.59	0.59	5	أو افق بشدة
8	تحسين استجابة الشركات الناشئة للهجمات الإلكترونية يسهم في تقليل التوقفات غير المخطط لها وتحسين الكفاءة التشغيلية.	4.57	0.55	6	أو افق بشدة
10	تبني تقنيات أمن سيبر اني متقدمة يعزز من استقرار الأنظمة التشغيلية لشركات الأمن السيبر اني الناشئة.	4.56	0.60	7	أو افق بشدة

م	العبارة	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الموافقة
7	تعزيز التزام الشركات بمعايير الأمن السيبراني يسهم في تحسين فعالية الفرق التقنية داخل الشركات الناشئة.	4.55	0.57	8	أوافق بشدة
13	الشركات الناشئة التي تعتمد على معايير الأمن السيبراني توفر بيئة أكثر استقرارًا للعملاء، مما ينعكس إيجابيًا على الكفاءة التشغيلية.	4.52	0.66	9	أوافق بشدة
4	تطبيق معايير الأمن السيبراني يعزز من قدرة الشركات على التكيف مع التغيرات التكنولوجية وتحسين كفاءتها التشغيلية.	4.51	0.60	10	أوافق بشدة
6	التزام الشركات الناشئة بمعايير الأمن السيبراني يعزز من مستوى الثقة بين العملاء، مما يساهم في تحسين الكفاءة التشغيلية.	4.51	0.62	11	أوافق بشدة
5	تخصيص موارد مالية لدعم تطبيق معايير الأمن السيبراني يعزز من الكفاءة التشغيلية للشركات الناشئة.	4.43	0.62	12	أوافق بشدة
9	اعتماد تقنيات حديثة لتحسين الأمان السيبراني يسهم في زيادة كفاءة التشغيل من خلال تعزيز الحماية ضد المخاطر المتزايدة.	4.40	0.80	13	أوافق بشدة
	المتوسط الحسابي العام	4.55	0.50		أوافق بشدة

يتضح من الجدول السابق ما يأتي: تظهر درجة موافقة أفراد الدراسة (من رؤساء الإدارات، ومديري الأقسام، والتقنيين) على عبارات محور "التزام شركات الأمن السيبراني الناشئة بتطبيق معايير الأمن السيبراني وتأثير ذلك على الكفاءة التشغيلية" من خلال درجات "موافق بشدة" على أداة الدراسة. تراوحت المتوسطات الحسابية بين(4.40 و4.67)، وهي تقع ضمن الفئة الخامسة من فئات المقياس المتدرج الخماسي، مما يشير إلى درجة "موافق بشدة" بالنسبة لأداة الدراسة.

كشف التحليل عن أن العبارة رقم (2) كانت الأعلى في المتوسط الحسابي (4.67)، وهي تشير إلى أن "التزام شركات الأمن السيبراني الناشئة بتطبيق معايير الأمن السيبراني يعزز من قدرة الشركة على تحسين كفاءتها التشغيلية". وهذا يدل على أهمية الالتزام بهذه المعايير لتحسين الكفاءة التشغيلية.

تلتها **العبارة رقم (1)**، والتي نصها "الشركات التي تلتزم بمعايير الأمن السيبراني تتمتع بقدرة أعلى على مواجهة التهديدات الإلكترونية، مما يزيد من كفاءتها التشغيلية" في **المرتبة الثانية**، بمتوسط حسابي (4.63).

ثم جاءت العبارة رقم **(11)**، "الدعم الحكومي لمعايير الأمن السيبراني يسهم بشكل كبير في تحسين الكفاءة التشغيلية لشركات الأمن السيبراني الناشئة"، في **المرتبة الثالثة**، بمتوسط حسابي (4.61).

بالإضافة إلى ذلك، كانت **العبارة رقم (3)**، "تطبيق معايير الأمن السيبراني يوفر بيئة آمنة للبيانات، مما يعزز من كفاءة العمليات التشغيلية"، في **المرتبة الرابعة**، بمتوسط حسابي (4.60)، مما يبرز دور البيئة الآمنة للبيانات في تعزيز كفاءة العمليات.

وجاءت **العبارة رقم (12)**، "الشركات الناشئة التي تلتزم بمعايير الأمن السيبراني تكون أكثر قدرة على توفير خدمات موثوقة، مما يسهم في تحسين الكفاءة التشغيلية"، في **المرتبة الخامسة**، بمتوسط حسابي 4.59.

وفي نفس السياق، كانت **العبارة رقم (8)**، "تحسين استجابة الشركات الناشئة للهجمات الإلكترونية يسهم في تقليل التوقفات غير المخطط لها وتحسين الكفاءة التشغيلية"، في **المرتبة السادسة**، بمتوسط حسابي (4.57).

تلتها **العبارة رقم (10)**، "تبني تقنيات أمن سيبراني متقدمة يعزز من استقرار الأنظمة التشغيلية لشركات الأمن السيبراني الناشئة"، في **المرتبة السابعة**، بمتوسط حسابي (4.56).

ثم جاءت **العبارة رقم (7)**، "تعزيز التزام الشركات بمعايير الأمن السيبراني يسهم في تحسين فعالية الفرق التقنية داخل الشركات الناشئة"، في **المرتبة الثامنة**، بمتوسط حسابي (4.55).

بينما جاءت **العبارة رقم (13)**، "الشركات الناشئة التي تعتمد على معايير الأمن السيبراني توفر بيئة أكثر استقرارًا للعملاء، مما ينعكس إيجابيًا على الكفاءة التشغيلية"، في **المرتبة التاسعة**، بمتوسط حسابي (4.52).

أما **العبارة رقم (4)**، "تطبيق معايير الأمن السيبراني يعزز من قدرة الشركات على التكيف مع التغيرات التكنولوجية وتحسين كفاءتها التشغيلية"، فقد احتلت **المرتبة العاشرة** بمتوسط حسابي (4.51).

تلتها **العبارة رقم (6)**، "التزام الشركات الناشئة بمعايير الأمن السيبراني يعزز من مستوى الثقة بين العملاء، مما يساهم في تحسين الكفاءة التشغيلية"، في **المرتبة الحادية عشرة** بمتوسط حسابي (4.51).

ثم جاءت **العبارة رقم (5)**، "تخصيص موارد مالية لدعم تطبيق معايير الأمن السيبراني يعزز من الكفاءة التشغيلية للشركات الناشئة"، في **المرتبة الثانية عشرة** بمتوسط حسابي (4.43).

وأخيراً، جاءت العبارة رقم (9)، "اعتماد تقنيات حديثة لتحسين الأمان السيبراني يسهم في زيادة كفاءة التشغيل من خلال تعزيز الحماية ضد المخاطر المتزايدة"، في المرتبة الثالثة عشر بمتوسط حسابي (4.40).

بناءً على ما سبق، يمكن استنتاج أن المتوسط العام لاستجابات أفراد الدراسة على عبارات محور "التزام شركات الأمن السيبراني الناشئة بتطبيق معايير الأمن السيبراني وتأثير ذلك على الكفاءة التشغيلية" بلغ(4.55 من 5)، مما يشير إلى درجة "موافق بشدة" على الأداة، مما يعكس تأكيد أفراد الدراسة على أن الالتزام بمعايير الأمن السيبراني له تأثير كبير على تحسين الكفاءة التشغيلية لشركات الأمن السيبراني الناشئة.

عرض وتفسير الجداول الخاصة بالفرض الرابع: توجد علاقة ذات دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين توجهات الأفراد في المجتمع السعودي، وبين استدامة شركات الأمن السيبراني الناشئة.

جدول رقم (12): المتوسطات الحسابية والانحرافات المعيارية لإجابات عينة الدراسة على عبارات العلاقة بين توجهات الأفراد في المجتمع السعودي واستدامة شركات الأمن السيبراني الناشئة

م	العبارة	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الموافقة
2	تزايد وعي الأفراد في المجتمع السعودي بأهمية الأمن السيبراني يدفع الشركات الناشئة إلى التوسع في خدماتها.	4.20	0.72	1	أوافق
1	زيادة ثقة الأفراد في خدمات الأمن السيبراني تعزز من فرص نجاح الشركات الناشئة ونموها المؤسسي.	4.43	0.68	2	أوافق بشدة
11	ارتفاع طلب الأفراد على الحلول الأمنية الرقمية يسهم في تطوير بنية الشركات الناشئة وتوسّعها.	4.45	0.65	3	أوافق بشدة
3	دعم الأفراد لخدمات الأمن السيبراني يعزز من الاستقرار المالي والتوسع التنظيمي للشركات الناشئة.	4.55	0.59	4	أوافق بشدة
12	انتشار الثقافة الرقمية لدى الأفراد يزيد من فرص نمو شركات الأمن السيبراني الناشئة في السوق المحلي.	4.40	0.71	5	أوافق بشدة
8	الميل المتزايد لاستخدام الأفراد للتقنيات الرقمية يدفع الشركات الناشئة لتطوير خدماتها الأمنية باستمرار.	4.50	0.62	6	أوافق بشدة
10	الاستجابة الإيجابية من الأفراد لحملات التوعية بالأمن السيبراني تساهم في توسع الشركات الناشئة.	4.41	0.69	7	أوافق بشدة
7	تفضيل الأفراد التعامل مع شركات ذات مستوى أمان مرتفع يعزز من مكانة الشركات الناشئة في السوق.	4.53	0.60	8	أوافق بشدة
13	اتجاهات الأفراد الإيجابية نحو الأمن السيبراني تشجع على استثمارات جديدة في هذا القطاع.	4.47	0.64	9	أوافق بشدة
4	توجهات الأفراد نحو حماية بياناتهم الشخصية تسهم في تنمية قدرات الشركات الناشئة الأمنية.	3.75	0.88	10	أوافق إلى حد ما
6	وعي الأفراد بتهديدات الفضاء السيبراني يسهم في دعم شركات الأمن السيبراني الناشئة وتوسعها.	4.05	0.80	11	أوافق بشدة
5	مشاركة الأفراد في تقييم خدمات الأمن السيبراني تعزز من تحسين الأداء المؤسسي للشركات الناشئة.	3.90	0.85	12	أوافق إلى حد ما
9	اعتماد الأفراد على الحلول الأمنية الوطنية يعكس ثقتهم بالشركات الناشئة ويحفز نموها.	4.40	0.71	13	محايد
	المتوسط الحسابي العام	4.54	0.71		أوافق بشدة

يتضح من الجدول السابق: يعكس جدول رقم (12) نتائج آراء أفراد العينة حول أثر توجهات الأفراد في المجتمع السعودي على استدامة شركات الأمن السيبراني الناشئة. وتشير النتائج إلى أن المتوسط الحسابي العام قد بلغ (4.54)، وهو ما يدل على درجة موافقة مرتفعة للغاية تعكس إجماعًا واضحًا من المشاركين على وجود علاقة إيجابية مؤثرة بين توجهات الأفراد واستدامة هذه الشركات.

أولًا: العبارات الأعلى تقييمًا:

جاءت العبارة (3) "دعم الأفراد لخدمات الأمن السيبراني يعزز من الاستقرار المالي والتوسع التنظيمي للشركات الناشئة" في المرتبة الرابعة بمتوسط حسابي (4.55) وانحراف معياري منخفض (0.59)، ما يدل على قناعة قوية لدى العينة بأن الدعم المجتمعي يُسهم مباشرة في استقرار ونمو هذه الشركات.

كما حصلت العبارة (11) "ارتفاع طلب الأفراد على الحلول الأمنية الرقمية يسهم في تطوير بنية الشركات الناشئة وتوسّعها" على المرتبة الثالثة بمتوسط (4.45) وانحراف معياري (0.65)، مما يعكس أن تزايد الطلب المجتمعي يعد قوة دافعة للتوسع الداخلي وتحسين البنية التحتية.

أما العبارة (1) "زيادة ثقة الأفراد في خدمات الأمن السيبراني تعزز من فرص نجاح الشركات الناشئة ونموها المؤسسي"، فجاءت في المرتبة الثانية بمتوسط (4.43) وانحراف معياري (0.68)، لتؤكد على أن الثقة المجتمعية في هذه الخدمات هي عنصر جوهري في تحقيق النمو المؤسسي.

وجاءت العبارة (2) "تزايد وعي الأفراد بأهمية الأمن السيبراني يدفع الشركات الناشئة إلى التوسع في خدماتها" احتلت المرتبة الأولى بمتوسط (4.20)، وهي مؤشر واضح على أن الوعي العام بات من محركات التوسع الاستراتيجي لهذه الشركات، رغم أنه جاء بأقل متوسط بين العبارات الـ10 الأولى.

كذلك، جاءت العبارة (12) "انتشار الثقافة الرقمية لدى الأفراد يزيد من فرص نمو شركات الأمن السيبراني الناشئة في السوق المحلي" في المرتبة الخامسة بمتوسط (4.40)، مما يؤكد على أن الثقافة الرقمية المجتمعية تخلق مناخًا مشجعًا لنمو هذه الشركات.

أما العبارة (8) "الميل المتزايد لاستخدام الأفراد للتقنيات الرقمية يدفع الشركات الناشئة لتطوير خدماتها الأمنية باستمرار" فقد حصلت على المرتبة السادسة بمتوسط (4.50) وانحراف (0.62)، مما يعكس ديناميكية واضحة في العلاقة بين استخدام التقنية وابتكار الخدمات.

ثانياً: عبارات ذات تقييم متوسط:

العبارة (10) "الاستجابة الإيجابية من الأفراد لحملات التوعية بالأمن السيبراني تساهم في توسع الشركات الناشئة"، حصلت على المرتبة السابعة بمتوسط (4.41)، ما يشير إلى أن الحملات التوعوية تؤدي دورًا فاعلًا، لكن هناك مجال لتعزيز تأثيرها.

العبارة (7) "تفضيل الأفراد التعامل مع شركات ذات مستوى أمان مرتفع يعزز من مكانة الشركات الناشئة في السوق"، جاءت في المرتبة الثامنة بمتوسط (4.53) وانحراف (0.60)، وهي قيمة مرتفعة وتدل على أن سمعة الأمان عنصر رئيسي في التنافس السوقي.

العبارة (13) "اتجاهات الأفراد الإيجابية نحو الأمن السيبراني تشجع على استثمارات جديدة في هذا القطاع" جاءت في المرتبة التاسعة بمتوسط (4.47)، مما يؤكد دور الفرد في تحفيز المناخ الاستثماري داخل قطاع الأمن السيبراني.

ثالثاً: العبارات الأقل تقييمًا

جاءت العبارة (4) "توجهات الأفراد نحو حماية بياناتهم الشخصية تسهم في تنمية قدرات الشركات الناشئة الأمنية" في المرتبة العاشرة بمتوسط (3.75) وانحراف معياري مرتفع نسبيًا (0.88)، ما يدل على تفاوت في الإدراك المجتمعي لأهمية حماية البيانات كمدخل لتطوير هذه الشركات.

العبارة (6) "وعي الأفراد بتهديدات الفضاء السيبراني يسهم في دعم شركات الأمن السيبراني الناشئة وتوسعها"، حازت على المرتبة الحادية عشرة بمتوسط (4.05)، ما يعني وجود اتفاق نسبي على أن الوعي بالمخاطر يعزز فرص النمو، لكن بدرجة أقل من العبارات الأخرى.

أما العبارة (5) "مشاركة الأفراد في تقييم خدمات الأمن السيبراني تعزز من تحسين الأداء المؤسسي للشركات الناشئة"، فقد جاءت في المرتبة الثانية عشرة بمتوسط (3.90)، ما يدل على أن هناك ضعفًا في مساهمة الأفراد في عمليات التقييم والمتابعة، وهي نقطة تتطلب تطوير قنوات المشاركة المجتمعية.

وأخيرًا، جاءت العبارة (9) "اعتماد الأفراد على الحلول الأمنية الوطنية يعكس ثقتهم بالشركات الناشئة ويحفز نموها" في المرتبة الأخيرة بمتوسط (4.40) رغم تقييم "محايد"، ما يشير إلى وجود تباين في آراء العينة بشأن العلاقة بين الثقة في الحلول المحلية والنمو الفعلي لهذه الشركات.

ثاني عشر: النتائج العامة للدراسة:

أسفرت الدارسة الحالية عن مجموعة من النتائج والتي أجابت بدورها على فروض الدارسة وهذه النتائج يمكن توضيحيا في الآتي:

أ- النتائج الخاصة بالفرض الأول: توجهات الأفراد نحو بعض المتغيرات الديموغرافية:

- يتضح من الجدول (1) أوضحت نتائج الدارسة أن معظم بلغت نسبة العاملين في شركات الأمن السيبراني الناشئة (Cipher، CQR، COGNNA) نحو 56% من إجمالي العينة، وهم من متخذي القرار في الإدارات العليا والوسطى إضافة إلى الموظفين في الأقسام التقنية. بينما بلغت نسبة مستخدمي خدمات هذه الشركات من الأفراد داخل المجتمع السعودي نحو 44.0%، وهو ما يعكس اهتمام الدراسة بقياس واقع الاستدامة من زاويتين: داخلية تمثّل العاملين، وخارجية تمثّل المستفيدين من الخدمات.
- يتضح من الجدول (2) أن غالبية عينة الدراسة من متخذي القرار ومستخدمي خدمات هذه الشركات كانوا من الذكور، وذلك بنسبة (70%) من مجتمع الدراسة، ونسبة (30%) من مجتمع الدراسة إناث، وهذا يدل على تنوع مجتمع الدراسة حيث تكون ممثلة لمجتمع البحث للتعامل مع مشكلات الأمن السيبراني ومواصلة جهود المملكة في تحقيق المساواة بين الجنسين.
- يتضح من الجدول (3) أن سنوات الخبرة العملية للعاملين في شركات الأمن السيبراني. جاء في الترتيب الأول: (أقل من 5 سنوات) بنسبة 50% وهي النسبة الأكبر من أفراد العينة لديهم من الخبرة العملية، مما يعكس الطبيعة الناشئة لشركات الأمن السيبراني في المملكة العربية السعودية، حيث أن العديد من هذه الشركات تعتبر حديثة العهد في السوق، تليها تتراوح سنوات الخبرة (من 5 إلى 10 سنوات) بنسبة 30%، وهذه الفئة تعكس الخبرة المتوسطة التي تكتسبها شركات الأمن السيبراني الناشئة في مرحلة التوسع والابتكار، وتليها الأفراد لديهم (أكثر من 10 سنوات) من الخبرة بنسبة 20%، ويعود ذلك إلى وجود بعض الأفراد الذين انتقلوا للعمل في شركات الأمن السيبراني من شركات أخرى قديمة ذات خبرة طويلة في المجال التقني.
- يتضح من الجدول (4) أوضحت نتائج الدراسة أن النسبة الأعلى من إجمالي أفراد الدراسة مؤهلهم العلمي بكالوريوس بنسبته مئوية (72%) وهي الفئة الأكبر من بين فئات الدراسة، يليها نسبته (24%) من إجمالي أفراد الدراسة مؤهلهم ماجستير، في حين وجد أن ما نسبته (2.7%) من إجمالي أفراد الدراسة دكتوراه، في حين وجد أن ما نسبته (1.3%) من إجمالي أفراد الدراسة مؤهلهم العلمي دبلوم، وهي الفئة الأقل من بين فئات الدراسة.

كشفت النتائج عن وجود فروق ذات دلالة إحصائية في توجهات الأفراد نحو خدمات الأمن السيبراني تعزى إلى المتغيرات الديموغرافية (العمر، الجنس، المستوى التعليمي، مستوى الاستخدام الرقمي). والذي يبين أن:

- الأفراد ذوي التعليم العالي والمهارات الرقمية المتقدمة أظهروا توجهات أكثر إيجابية.
- الفئات العمرية الشابة كانت أكثر وعيًا واهتمامًا باستخدام هذه الخدمات.
- كما سجلت فروق واضحة بين الجنسين لصالح الذكور في بعض المؤشرات، وإن كانت غير كبيرة.

ب- النتائج الخاصة بالفرض الثاني:

أظهرت نتائج الجدول الخاص بالفرض الثاني، والذي حلل واقع تطبيق معايير الأمن السيبراني وبين الفاعلية التنظيمية لشركات الأمن السيبراني الناشئة، أن الشركات الناشئة تطبق بدرجة عالية أدوات وتقنيات متقدمة للأمن السيبراني. حيث تراوح المتوسط الحسابي بين (4.41 إلى 4.80)، بمعدل عام (4.65) يقع ضمن درجة "موافق بشدة" وفق مقياس ليكرت. أبرزت النتائج أن:

- الشركات تولي أهمية لتطبيق أدوات وتقنيات حديثة.
- هناك التزام بالمعايير العالمية مثل.ISO 27001
- يتم توفير تدريب مستمر للموظفين، واعتماد خطط واضحة للاستجابة للحوادث.
- استخدام الحماية السحابية وحلول الشبكات يشيع بين الشركات، ما يعكس استعدادها لمواجهة التهديدات السيبرانية بكفاءة.

وهذا يؤكد على العلاقة القوية بين الالتزام بمعايير الأمن السيبراني وفاعلية الأداء التنظيمي لهذه الشركات، مما يعزز من فرص استدامتها.

ج- نتائج اختبار الفرض الفرعي الثالث:

لاختبار صحة الفرض الفرعي الأول أظهرت البيانات وجود علاقة قوية ذات دلالة إحصائية بين توجهات الأفراد (الوعي، ودرجة الثقة، ودوافعهم) لاستخدام خدمات الأمن السيبراني وبين دعم الكفاءة التشغيلية لشركات الأمن السيبراني. وقد عكست النتائج ارتفاعًا ملحوظًا في درجات الوعي والثقة، إلى جانب دوافع استخدام واضحة تعكس اهتمام المجتمع بحماية بياناته وأنشطته الرقمية، مما يؤكد أن تلك التوجهات تُعد عاملاً حاسمًا في تعزيز فعالية الخدمات الأمنية الرقمية.

د- نتائج اختبار الفرض الفرعي الرابع:

أظهرت النتائج إلى وجود علاقة ذات دلالة إحصائية توجهات الأفراد في المجتمع السعودي، وبين استدامة شركات الأمن السيبراني الناشئة. إذ تبيّن أن ارتفاع الطلب المجتمعي وازدياد الثقة بتلك الخدمات يساهمان في دعم التوسع المؤسسي، وتحفيز بيئة الابتكار، وجذب الاستثمارات، مما يسهم بشكل مباشر في استدامة هذه الشركات على المدى الطويل.

هـ- نتائج اختبار الفرض الرئيسي:

أظهرت نتائج التحليل الإحصائي وجود علاقة ذات دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين توجهات الأفراد في المجتمع السعودي نحو خدمات الأمن السيبراني، وواقع استدامة شركات الأمن السيبراني الناشئة في المملكة العربية السعودية. ويشير ذلك إلى أن مدى وعي وثقة ودوافع الأفراد تجاه هذه الخدمات ينعكس بشكل مباشر على استمرارية ونمو تلك الشركات.

الاستنتاج العام:

وأوضحت النتائج المترتبة على فرضيات الدراسة إلى وجود ترابط متين بين توجهات الأفراد نحو الأمن السيبراني، ومدى تطبيق الشركات الناشئة للمعايير والسياسات الأمنية، مما يسهم بشكل مباشر في نمو واستدامة هذا القطاع الحيوي في المملكة. وتوصي الدراسة بضرورة تعزيز الوعي المجتمعي، والاستثمار في رأس المال البشري، وتحديث التشريعات بما يتماشى مع التطورات التقنية لحماية الفضاء الرقمي وتعزيز بيئة ريادة الأعمال في مجال الأمن السيبراني.

من خلال تحليل نتائج الدراسة المتعلقة باستخدام تقنيات الأمن السيبراني في الشركات الناشئة بالمملكة العربية السعودية، نجد أن نتائج أفراد العينة تشير إلى موافقة قوية على أن هذه الشركات تبذل جهدًا كبيرًا في تطبيق وتبني أحدث تقنيات الأمن السيبراني لحماية أنظمتها وبياناتها من المخاطر السيبرانية. وقد حصلت معظم العبارات على درجات "موافق بشدة" في مقياس ليكرت، مما يعكس التزام الشركات بدمج هذه التقنيات في عملياتها التشغيلية.

وأكدت الأبحاث التي تؤكد أن الشركات الصغيرة والمتوسطة (SMES) عرضة بشكل خاص للتهديدات السيبرانية، وتحتاج إلى استراتيجيات أمنية مخصصة، تأتي هذه الدراسة لتدعم ذلك التوجه. فقد كشفت أبحاث سابقة أيضًا عن أن طموحات هذه الشركات، ومواردها، ومستوى معرفتها بالأمن السيبراني غالبًا ما تكون محدودة أو غير كافية (Zawaideh et al., 2023). ومع توفر المنتجات والتقنيات الحالية، فإن أنظمة الأمن السيبراني المطبقة في الشركات الصغيرة والمتوسطة تُعد باهظة التكاليف ومعقدة عند مقارنتها بالحلول الأمنية المتقدمة الموجهة عادةً للمؤسسات الكبرى. وتتوافق نتائج هذه الدراسة مع ما أظهرته الأبحاث السابقة التي تناولت الشركات الصغيرة والمتوسطة (SMEs) باعتبارها فئة هشة أمام التهديدات السيبرانية، مما يتطلب حلولاً أمنية مصممة خصيصًا لتناسب خصائصها ومواردها المحدودة .(Rodriguez-Baca et al., 2022) غير أن هذه الدراسة تميزت عن غيرها من الدراسات السابقة بقدرتها على سد فجوة واضحة في الأدبيات العلمية من خلال دمج تقنيات الذكاء الاصطناعي كأداة مبتكرة لمعالجة غياب الحلول الأمنية المخصصة التي يسهل تطبيقها وبتكلفة ملائمة لهذه الفئة من الشركات.

ثالث عشر: التوصيات والمقترحات:

1- ضرورة أن تدعم الجهات الحكومية تطوير معايير وسياسات الأمن السيبراني، وذلك من خلال تحديث الأطر التنظيمية بما يواكب التحديات الحديثة، مع قيام صُنّاع القرار بوضع تشريعات تضمن حماية البيانات الشخصية وتُشجع على الاعتماد الآمن على الخدمات السيبرانية.

2- وضع خطة وطنية شاملة للبيئة الرقمية والأمن السيبراني، تتضمن تطوير البنية التحتية لتقنيات المعلومات، وتعزيز قدرات الشبكات الرقمية، بما يسهم في توفير بيئة آمنة ومحفزة لتوسع الشركات الناشئة في هذا المجال.

3- تشجيع الاستثمارات في تقنيات الذكاء الاصطناعي والأمن السيبراني، من خلال حوافز حكومية ودعم برامج الابتكار، مما يعزز من جاهزية الشركات الناشئة لمواجهة التهديدات المتزايدة واستدامتها على المدى الطويل.

4- ضمان حماية الخصوصية والملكية الفكرية للمستخدمين، وذلك عن طريق سنّ تشريعات واضحة تضمن عدم إساءة استخدام المعلومات الشخصية، بما يعزز الثقة بين الأفراد ومزودي خدمات الأمن السيبراني.

قائمة المراجع:

أولاً: المراجع العربية:

- أسامة طلعت (2021). ما هي الشركة الناشئة (Startup) وصفاتها وكيفية تمويلها، موقع الرابحون ، https://www.alrab7on.com/what-is-a-startup/.
- آل مداوي، علي (2023). الأمن السيبراني: تعريفه- أهميته- أنواعه– استراتيجيات الوقاية من الهجمات السيبرانية، وزارة الخارجية - معهد الأمير سعود الفيصل للدراسات الدبلوماسية.
- البغدادي، مروة فتحي السيد (2021) اقتصاديات الأمن السيبراني في القطاع المصرفي، مجلة البحوث القانونية والاقتصادية.
- البلادي، سلمه وعثمان، فتون (2023) الدور الفعال للبيانات الضخمة في دعم قطاع الاتصالات: دراسة تحليلية مجلة دراسات المعلومات والتكنولوجيا: (1-16).
- تغريد صفاء، لبنى خميس مهدي (2020). أثر السيبرانية في تطور القوة، مجلة حامورابي للدراسات، بغداد، مركز حمورابي للبحوث والدراسات الاستراتيجية، ع 33 34 ، ص 149.
- تقرير Forbes Middl East (2022). واقع الابتكار الوطني الشريكات الأكثر ابتكاراً في السعودية، هيئة تنمية البحث والتطوير والابتكار.
- تقرير الاستدامة (2023). النهوض بالاستدامة اليوم لبناء غد أفضل.
- تقرير الإنترنت السعودية (2023). هيئة الاتصالات والفضاء والتقنية.
- تقرير الكتاب السنوي للتنافسية العالمية لعام 2022 الصادر عن مركز التنافسية العالمي التابع للمعهد الدولي للتنمية الإدارية في سويسرا IMD.
- جناوي، عبد العزيز .(2018) قراءة فيسوسيولوجيا مخاطر الحداثة الانعكاسية، مجلة دراسات وأبحاث، م 30، ع 30.
- حسين بن سليمان بن رشد الطيار(2020) ، الأمن السيبراني في منظور مقاصد الشارع: دراسة تأصيلية، المملكة العربية السعودية، جامعة الطائف، مجلة جامعة الطائف للعلوم الإنسانية، المجلد 6، العدد 2
- خالد، دلال ويعقوب، منذر (2021). تأثير إسعاد الزبون في الحصة السوقية للشركة دراسة استطلاعية في متجر فاملي مول في محافظة دهوك، مجلة تكريت للعلوم الإدارية والاقتصادية، مجلد (17) 55 (553-566)
- خليل، هشام محمد (2012). الجوانب الإجرامية للجوانب المعلوماتية، مجلس الأمن والقانون، عدد 2، شرطة. دبي.
- السمحان، مني عبد الله (2022). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، 111.
- الشريفي، علي. (2019). دور التوجه الاستراتيجي في السمعة الاستراتيجية وتأثيره في الضغوط التنافسية دراسة استطلاعية في شركات الاتصال المتنقلة في العراق، مجلة الاقتصاد والعلوم الإدارية، المجلد 25 (113): (191-220).
- صاح مهدي هادي الشمري، زيد محمد علي إسماعيل (2020). الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية، العراق، مجلة قضايا سياسية، العدد 68 ، جامعة النهرين، كلية العلوم السياسية، ص 277.
- عادل رؤى ويعقوب، منذر. (2022). التوجه الإبداعي ودوره في زيادة الحصة السوقية دراسة استطلاعية لآراء عينة من زبائن شركة صدف للأثاث في مدينة دهوك، مجلة اقتصاديات الأعمال للبحوث التطبيقية، مجلد 3 (6)
- عزت، محمود (2018). الفضاء السيبراني وتحديات الأمن المعلوماتي العربي، المجلة العربية العدد 498.
- العطوى، حكيم (2021). دور وأهمية ثقافة حوكمة الشركات على استدامة الشركات الناشئة: دراسة ميدانية، مجلة إدارة الأعمال والدراسات الاقتصادية، المجلد 7, العدد 2.
- فتوح، وسام حسن (2021). الأمن السيبراني في المنطقة العربية: توعية المصارف المؤسسات المالية لإتباع المعايير العالمية، مجلة اتحاد المصارف العربية، العدد (490).
- مداخل زيد عبدالرحيم التيماني (2021). واقع الوعي المعلوماتي بالأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بالأمن السيبراني
- المنيع، الجوهرة (2022). متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية 2030، المجلة العلمية، المجلد 38، العدد1.
- الهيئة الوطنية للأمن السيبراني (2023). الإطار التنظيمي لتراخيص خدمات مراكز عمليات الأمن السيبراني المدارة.

ثانياً: المراجع الأجنبية:

- Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. Decision Support Systems,. https://doi.org/10.1016/j.dss.2021.113580
- Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. Business Horizons, 63(4), 531–540.
- GAELLE, Dis, c'est quoi une start-up..., wydden ,2019, juillet 14, Consulté le 15/02/2021, https://wydden.com/dis-cest-quoi-une-start-up/.
- GRAHAM P, STARTUP=GROWTH, 2012, September, PAUL GRAHAM, Consulté le 18/02/2021 http://www.paulgraham.com/growth.html.
- Jayathilaka, H. M. T. N., & Wijayanayake, J. (2024). Systematic literature review on developing an AI framework for SME cybersecurity identification and personalised recommendations. The Journal of Desk Research Review and Analysis, 2(1), 249–250.
- larousse, Consulté le 10/01/2021, https://www.larousse.fr/dictionnaires/francais/startup/ 74493.
- National institute of standards and technology (NIST) (2018), a Glossary of key information security terms National institute of standards and technology interagency or internal report. available at http://csrc.nist.gov/publications.
- Pierre Facon, Qu'est-ce qu'une start-up ? Tout ce qu'il faut savoir, Le Coin des Entrepreneurs, Consulté le 13/03/2021,https://www.lecoindesentrepreneurs.fr/start-up-definition-particularites/.
- Ramirez, M, Ariza, L., and Miranda, M., (2022). The disclosure of information on rsecurity in listed companies in Latin America-proposal for a cyber security disclosure index), journal of sustainability, 14(3.)
- Rea-Guaman, A. M., Mejía, J., San Feliu, T., & Calvo-Manzano, J. A. (2020). AVARCIBER: A framework for assessing cybersecurity risks. Cluster Computing, 23(3).
- Rodriguez-Baca, L. S., Larrea-Serquen, R. L., Cruzado, C. F., Alarcon-Diaz, M., Garcia- Hernandez, S. E., & Pebe-Espinoza, J. (2022). Business Cybersecurity. Case study in Peruvian and Mexican SMEs. 2022 3rd International Conference for Emerging Technology, INCET 2022.
- Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. In SN Computer Science (Vol. 2, Issue 3). Springer.
- Shojaifar, A., Fricker, S. A., & Gwerder, M. (2020). Automating the Communication of Cybersecurity Knowledge: Multi-Case Study.
- Zawaideh, F. H., Abu-Ulbeh, W., Mjlae, S. A., El-Ebiary, Y. A. B., Al Moaiad, Y., & Das, S. (2023). Blockchain Solution For SMEs Cybersecurity Threats In E-Commerce. 2023 International Conference on Computer Science and Emerging Technologies, CSET 2023. https://doi.org/10.1109/CSET58993.2023.10346628