

جامعة ميدأوشن

كلية الإدارة

قسم / تخصص ادارة المخاطر



سُبُل مساعدة لإدارة مخاطر الأمن السيبراني في الشركات السعودية التقنية بحسب تشريعات الهيئة الوطنية
للأمن السيبراني

Ways to help manage cybersecurity risks in Saudi technology companies according to the legislation of
the National Cybersecurity Authority

إعداد الطالبة/

هُتاف بنت عبدالله خليل

إشراف/

د. وليد عبدالجواد سليمان صديق

د. الفيصّل عبدالحميد محمد حسن

العام الدراسي:

2023

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

الإهداء،،

إلى من أبصرتُ بها الحياة، واستمدت منها القُوَّة والمثابرة والكِفاح
إلى الشامخة التي علّمتني معنى الإصرار على الازدهار، إلى ينبوع العطاء والحنان ..
إلى من دَفَعَتني بِقُوَّة على طريق العِلْم والنجاح، إلى مَنْ مهَّدت لي الصواب
وبوركت خطواتي بدعائها الذي أُجني ثماره في كُلِّ حينٍ وأن ..
إلى آمالي،، ساكنة الروح والأنفاس
إلى أُمِّي الغالية -رحمها الله-

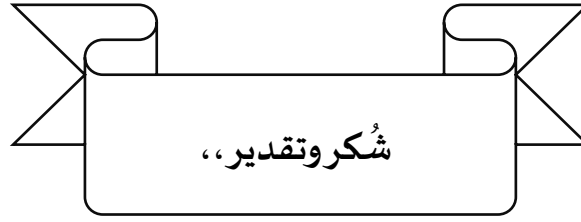
إلى مَنْ علّمني أن ارتقي سلم الحياة بِحِكْمَةٍ وصبر
إلى مَنْ بلّغني واوصاني على ذكر الله وشُكره في كل وقت
إلى برِّ الأمان، إلى مَنْ مَنَحَني الثقة ومكَّن لي السُّبُل ..
إلى سندي، ومَدَدَني، ومُهَجَّة حياتي
إلى والدي الغالي -بارك الله فيه-

إلى صديق الروح، ورفيق الجَل والترحال
إلى الداعم المُسَخَّر ..

إلى كُلِّ من ساندني

بُنُصْحٍ، وعِلْمٍ، وإشادةٍ، ودُعاء

أهديكم هذا العمل المتواضع، راجيةً من الله تعالى أن يُمُنَّ علينا بعونه وتوفيقه



الحمد لله والشُّكر له -سُبْحَانَهُ- فَهُوَ الْمُنْعَمُ وَالْمُتَفَضِّلُ قَبْلَ كُلِّ شَيْءٍ، أَشْكُرُهُ وَاحْمَدُهُ عَلَى أَنْ حَقَّقَ لِي مَا أَصْبَوُ إِلَيْهِ
فِي اسْتِكْمَالِ دَرَجَةِ الْمَاجِسْتِيرِ فِي تَخْصِصِ إِدَارَةِ الْمَخَاطِرِ

ثُمَّ الْحَمْدُ لِلَّهِ الَّذِي سَخَّرَ فِي طَرِيقِي الْقَائِدَ الْمُتَمِّمَ الْأَسْتَاذَ / طَلالَ صَالِحِ الْحَرَبِيِّ إِذْ أَمَدَنِي بِوَأْفَرِ الدَّعْمِ وَاکْرَمَنِي
بِالتَّوْجِيهِ النَّاصِحِ وَسَهَّلَ لِي الطَّرِيقَ، فَلَهُ مَنِي بِلِيغِ الشُّكْرِ وَالْإِمْتِنَانِ ..

عَظِيمِ الشُّكْرِ وَالتَّقْدِيرِ لِكُلِّ اساتذتي الْكَرَامِ فِي جَامِعَةِ مِيدَاوُشْنِ، وَفَرِيقِ الدَّعْمِ الْفَنِيِّ

جَزَاهُمْ اللَّهُ عَنَّا خَيْرَ الْجَزَاءِ عَلَى كُلِّ جُهْدٍ بَذَلُوهُ، وَكُلِّ مَاقْدَمٍ مَوَّهَ لَنَا بِإِحْسَانٍ

كَمَا اخْصَ بِالذِّكْرِ وَالْعُرْفَانِ مُشْرِفِينَ هَذَا الْبَحْثَ الْعِلْمِيَّ

د. وَلِيدُ عَبْدِ الْجَوَادِ سَلِيمَانَ صَدِيقٍ

د. الْفَيْصَلُ عَبْدِ الْحَمِيدِ مُحَمَّدَ حَسَنَ

زَمَلَانِي الْأَعْزَاءُ،، لَكُمْ مِنِّي جَمِيعًا وَافِرِ الشُّكْرِ وَالْعُرْفَانِ

الْبَاحِثَةُ

هُتَافُ عَبْدِ اللَّهِ خَلِيلٍ

المستخلص:

سُبل مساعدة لإدارة مخاطر الأمن السيبراني في الشركات السعودية التقنية بحسب تشريعات الهيئة الوطنية للأمن السيبراني.

هدفت الدراسة إلى التعرف على سُبل مساعدة لإدارة مخاطر الأمن السيبراني في الشركات السعودية التقنية بحسب تشريعات الهيئة الوطنية للأمن السيبراني. وقد استخدمت الدراسة المنهج الوصفي التحليلي وأداة الاستبانة. وتمثل مجتمع الدراسة في منسوبي المؤسسات التكنولوجية في منطقة شرق الرياض والبالغ عددهم (370) موظف وموظفة. وبلغت حجم عينة الدراسة (120) مفحوص من منسوبي المؤسسات التكنولوجية في منطقة شرق الرياض. وتم اختيار العينة بالطريقة العشوائية عن طريق وضع الأسماء على جهاز الحاسب الآلي والاختيار من بينها، وقامت الباحثة بتصميم إستبانة إلكترونية لتحقيق أهداف الدراسة. وقد توصلت الدراسة إلى نتائج هامة ومنها: ان عبارات محور أهمية الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني، جاءت بدرجة (مرتفعة) حيث بلغ المتوسط الحسابي الكلي (3.73 من 5) وهو متوسط يقع ضمن الفئة الرابعة من فئات مقياس ليكرت الخماسي (3.40 إلى 4.19) وهي الفئة التي تشير إلى درجة (مرتفعة). إن هناك تفاوت في استجابات أفراد عينة الدراسة على عبارات محور طرق تطوير ادارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني، حيث تراوحت المتوسطات ما بين (3.52 إلى 3.86 من 5) وهي متوسطات تقع ضمن الفئة الرابعة من فئات مقياس ليكرت الخماسي وتشير إلى درجة (مرتفعة). ومن التوصيات التي وضعتها الدراسة: يجب أن تكون المؤسسات ملتزمة بتعزيز التوعية وتوفير التدريب المستمر للموظفين بشأن مخاطر الأمن السيبراني وتطوير أفضل الممارسات للوقاية منها. كما ينبغي تعزيز الوعي بمفهوم حماية المعلومات الحساسة وتحذير الموظفين من التهديدات السيبرانية المحتملة مثل الهجمات الاجتماعية والرسائل الاحتيالية.

الكلمات المفتاحية:

سبل/لإدارة/مخاطر/الأمن السيبراني/ التقنية/ الهيئة الوطنية للأمن السيبراني.

Abstract:

Ways to help manage cybersecurity risks in Saudi technology companies according to the legislation of the National Cybersecurity Authority

The study aimed to identify ways to help manage cybersecurity risks in Saudi technology companies in accordance with the legislation of the National Cybersecurity Authority. The study used the descriptive analytical method and the questionnaire tool. The study population was represented by employees of technological institutions in the eastern Riyadh region, who numbered (370) male and female employees. The size of the study sample was (120) examined from employees of technological institutions in the eastern Riyadh region. The sample was selected randomly by placing the names on the computer and choosing from among them. The researcher designed an electronic questionnaire to achieve the objectives of the study. The study reached important results, including: The statements on the importance of adhering to the legislation of the National Cybersecurity Authority came in at a high level, as the overall arithmetic mean reached (3.73 out of 5), which is an average that falls within the fourth category of the five-point Likert scale (3.40 to 4.19). It is the category that indicates a degree of (high). There is a discrepancy in the responses of the study sample members to the statements of the axis of methods for developing cybersecurity risk management in accordance with the legislation of the National Cybersecurity Authority, where the averages ranged between (3.52 to 3.86 out of 5), which are averages that fall within the fourth category is a five-point Likert scale and indicates a degree of (high). Among the recommendations developed by the study: Organizations must be committed to enhancing awareness and providing continuous training to employees on cybersecurity risks and best practices to prevent them. Awareness of protecting sensitive information should be enhanced and employees should be warned of potential cyber threats such as social attacks and email phishing.

key words:

Ways/management/risks/cybersecurity/technology/National Cybersecurity Authority

فهرس المحتوى:

الموضوع	الصفحة
صفحة العنوان	-
صفحة البسمة	ب
الإهداء	ج
الشكر والتقدير	د
ملخص البحث باللغة العربية	هـ
ملخص البحث باللغة الإنجليزية	و
قائمة المحتويات	ز
قائمة الجداول	ح
قائمة الأشكال	ي
قائمة الملاحق	ل
الفصل الأول: مقدمة الدراسة	1
مقدمة الدراسة	1
مشكلة الدراسة	2
أهمية الدراسة	3
أهداف الدراسة	5
أسئلة الدراسة	5
الدراسات السابقة	5
المنطلقات النظرية للدراسة	9
المنهجية وطرق البحث الأخرى	11
حدود البحث	13

14	الفصل الثاني: أدبيات الدراسة
14	1- مفهوم الأمن السيبراني
15	2- أهمية الأمن السيبراني
16	3- أهداف الأمن السيبراني
17	4- العناصر الأساسية للأمن السيبراني :
20	5- عوامل تحقيق الأمن السيبراني
21	6- مخاطر الأمن السيبراني
24	7- أهمية تشريعات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية
25	8- سبل تعزيز الأمن السيبراني في المملكة العربية السعودية :
28	الفصل الثالث: إجراءات البحث (المنهجية والإجراءات)
28	3-1: منهج البحث
28	3-2: مجتمع وعينة البحث
29	3-3: أداة البحث
30	3-4: صدق أداة البحث
31	3-5: ثبات أداة البحث
32	3-6: الأساليب الإحصائية
34	الفصل الرابع: نتائج الدراسة الميدانية
34	4-1: مقدمة:
34	4-2: خصائص عينة الدراسة
40	4-3: نتائج الدراسة الميدانية
48	الفصل الخامس: خلاصة لأهم نتائج الدراسة وتوصياتها

48	1-5: خلاصة الدراسة
49	2-5: نتائج الدراسة
50	3-5: توصيات الدراسة
51	4-5: مقترحات الدراسة
53	المراجع
53	المراجع العربية
55	المراجع الأجنبية
56	الملاحق

قائمة الجداول :

الجدول	الصفحة
جدول رقم (1-3) مقياس ليكرت الخماسي	29
جدول رقم (2-3) معاملات ارتباط بيرسون بين درجات كل فقرة والدرجة الكلية للبعد الذي تنتهي إليه.	30
جدول رقم (3-3) معاملات الارتباط بين درجة كل بعد والدرجة الكلية للاستبانة.	31
جدول رقم (4-3) معاملات ثبات أداة الدراسة.	32
جدول (3-5) الوزن النسبي للدرجات.	33
جدول (3-6) المتوسط المرجح للدرجات	33
جدول (1-4) توزيع عينة الدراسة حسب العمر	34
جدول (2-4) توزيع عينة الدراسة حسب المؤهل العلمي	35
جدول (3-4) توزيع عينة الدراسة حسب المستوى الوظيفي	36
جدول (4-4) توزيع عينة الدراسة حسب الخبرة العملية	37
جدول (5-4) توزيع عينة الدراسة حسب مجال العمل/ التخصص	38
جدول (6-4) المتوسطات الحسابية والانحرافات المعيارية لأبعاد سبل مساعدة لإدارة مخاطر الأمن السيبراني في الشركات السعودية التقنية بحسب تشريعات الهيئة الوطنية للأمن السيبراني	39
جدول (7-4) المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات اسباب مخاطر الأمن السيبراني في المملكة العربية السعودية مرتبة تنازليا حسب المتوسطات الحسابية.	40
جدول (8-4) المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات أهمية الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني مرتبة تنازليا حسب المتوسطات الحسابية.	43
جدول (9-4) المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات طرق تطوير ادارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني مرتبة تنازليا حسب المتوسطات الحسابية.	45

الفصل الأول

المقدمة:

لا شك بأن تنوع وسائل الاتصالات وتفاوت خصائصها وطبيعتها زاد من حجم تبادل المعلومات بين العالم بشكل كبير تسبب في زيادة العبء على الدول التي تسعى إلى تحقيق وتعزيز الأمن للفرد والمجتمع تحت ظل الاستخدام الواسع للحاسب الآلي وتطبيقاته، بالإضافة إلى الأجهزة الذكية وما يندرج تحتها؛ حيث شكّل الأمن على مر التاريخ الهاجس الأكبر للدول التي اعتبرت ضمان بقائها واستمرارها من بين أولويات سياستها، فالأمن هدف تسعى إليه كافة الدول كونه أحد أهم مقومات الحياة الانسانية، وأمام هذا الاحتياج الملح يبرز دور الأفراد والدولة، بالإضافة إلى المؤسسات والمنظمات الإقليمية والعالمية في توفية الحماية الأمنية (الخالدي، 2016، ص 52-53).

إن تشريعات الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية تهدف إلى تعزيز وحماية أمان البنية التحتية السيبرانية في المملكة، بالإضافة إلى حماية المعلومات الحساسة والتحقق من سلامة وتوافر وسرية البيانات المتداولة. كما أنه يتعين على المنظمات تحديد وتحليل المخاطر المحتملة لأمن البيانات والأنظمة الخاصة بها؛ حيث يتطلب ذلك إلى تقييم وتحليل التهديدات المحتملة والثغرات الأمنية بدراسة تأثيرها المحتمل على المنظمة، بالإضافة إلى وجوب الامتثال بتشريعات الهيئة الوطنية للأمن السيبراني عن طريق تطبيق سياسات الأمان والوصول والتحقق من الهوية وحماية الأنظمة وأجهزة معالجة المعلومات، وتأمين الشبكات والتدريب على وعي الأمن السيبراني (الغامدي، 2021، ص 17-18).

ونظرًا لأهمية الأمن السيبراني في العصر الحديث، فقد أصدر أمر ملكي كريم بإنشاء الهيئة الوطنية للأمن السيبراني، ترتبط بمقام خادم الحرمين الشريفين، وتضع الهيئة في أولوياتها استقطاب الكوادر الوطنية المؤهلة والطموحة وتأهيلها وتمكينها، بالإضافة إلى بناء الشراكات مع الجهات العامة والخاصة، وتحفيز الابتكار والاستثمار في مجال الأمن السيبراني للإسهام في تحقيق تقنية تخدم مستقبل الاقتصاد الوطني للمملكة العربية السعودية. كما تهدف الهيئة الوطنية للأمن السيبراني إلى تعزيز حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة معالجة البيانات والبرمجيات وماتقدمه من خدمات، وماتحويه من بيانات، مراعية في ذلك الأهمية الحيوية المتزايدة للأمن السيبراني في حياة المجتمعات، ومستهدفة التأسيس لصناعة وطنية في مجال الأمن السيبراني تُحقق الريادة في هذا المجال انطلاقًا مما تضمنته رؤية المملكة العربية السعودية 2023 (الهيئة الوطنية للأمن السيبراني، 2018، ص 96-97).

ويمثل الأمن الوطني أحد المقومات الأساسية لنجاح عملية التنمية، والنمو، والارتقاء بمختلف المجالات؛ حيث يعد الابداع الفكري، والذهني، والتخطيط المنظم، والسليم، والمثابرة العلمية، من أهم ركائز التنمية، ولا يتحقق الازهار لمشروع التنمية إلا في ظل وجود أمن راسخ يدعم ويُتيح وجود هذه الركائز، مما يُمكن الانسان من الاطمئنان على ذاته، وثروته، واستثماراته (الشراري، 2017، ص 88).

يتضح مما سبق أنه يتعين بل يجب على المنظمات وضع خطط استجابة للحوادث الأمنية وتنفيذها عند حدوث نوع من الانتهاكات الأمنية؛ ويشمل ذلك التعامل مع الاختراقات والتهديدات المحتملة واستعادة الأنظمة وتحليل الحوادث السيبرانية ونحوها لتعزيز الأمان في المستقبل. حيث تشترط تشريعات الهيئة الوطنية للأمن السيبراني الامتثال

للمعايير والارشادات الأمنية المعترف بها عالميًا؛ ومراجعة سياساتها واجرائتها بشكل دوري للتأكد من الامتثال لهذه المعايير واشعار الهيئة بالانتهاكات الأمنية واخذ الاجراء المناسب.

تتناول الباحثة في هذه الدراسة موضوع سبل مساعدة لادارة مخاطر الأمن السيبراني في الشركات السعودية الخاصة بحسب تشريعات الهيئة الوطنية للأمن السيبراني، عن طريق عمل دراسة عينة تطبيقية لبعض من المؤسسات التكنولوجية بمنطقة الرياض.

مشكلة الدراسة:

تتمثل مشكلة الدراسة الحالية في أنه يتعين على المنظمات تعزيز التوعية الأمنية لدى الموظفين وتوفير التدريب المناسب لهم بشأن مخاطر الأمن السيبراني وكيفية التعامل معها. ويُمكن أن يشمل ذلك التعريف بالتهديدات السيبرانية المحتملة وطرق الوقاية منها والابلاغ عن حالات الانتهاكات الأمنية. كما يجب على المنظمات اجراء تقييمات دورية لتحقيق من امتثالها بتشريعات الهيئة الوطنية للأمن السيبرانية ومراجعة المعايير الأمنية المعمول بها. حيث يشمل ذلك تنفيذ عمليات التدقيق الداخلي والتقييم الخارجي من مستوى الامتثال وتحديد نقاط الضعف التي تحتاج إلى تحسين. ولقد أصبح لأمن المعلومات في عصر التكنولوجيا الدور الأكبر في تحقيق التميز المؤسسي من خلال حماية البيانات و صد ومنع أي هجوم إلكتروني قد تتعرض له أنظمة الدولة المختلفة، بالإضافة إلى حماية الأنظمة التشغيلية من محاولات الولوج بشكل غير مسموح به لأهداف غير سليمة، وهو السبب وراء الأمر الملكي بإنشاء الهيئة الوطنية للأمن السيبراني (الخالدي، 2016، ص 41).

حيث ينتهج الأمن السيبراني الناجح نهجا معيناً يتكون عادة من طبقات متعددة للحماية تنتشر في أجهزة الكمبيوتر أو الشبكات أو البرامج أو البيانات المراد الحفاظ على سلامتها، وفي أي منظمة يجب على المستخدمين والعمليات وكذلك التكنولوجيا أن يتكاتفوا لإنشاء خط دفاع فعال من الهجمات السيبرانية عن طريق تنفيذ متطلبات تعزيز الأمن السيبراني (عبد ربه، 2020، ص 63).

فقد أكدت نتائج دراسة والدو Waldo (2017، ص 13) أنه يجب على المستخدمين فهم مبادئ أمن البيانات الأساسية والامتثال لها مثل اختيار كلمات مرور قوية، والحذر من المرفقات ذات المصدر المجهول في البريد الإلكتروني، والحرص على عمل نسخ احتياطية للبيانات.

عليه يتضح مما سبق أن الامتثال لتشريعات الهيئة الوطنية للأمن السيبراني يساهم على التعاون في تعزيز القدرة على التصدي للتهديدات السيبرانية وتعزيز الأمن السيبراني على المستوى الوطني. حيث تشجع تشريعات الهيئة الوطنية للأمن السيبراني على التطوير المستمر والابتكار في مجال الأمن السيبراني. ويجب على المنظمات مواكبة التطورات التكنولوجية وتحديث استراتيجياتها وتقنياتها الأمنية لمواجهة التهديدات السيبرانية الجديدة والمتقدمة.

ومن هذا المنطلق يمكن تحديد مشكلة الدراسة في التساؤل الرئيسي التالي: ماهي السبل المساعدة لادارة مخاطر الأمن السيبراني في الشركات السعودية الخاصة بحسب تشريعات الهيئة الوطنية للأمن السيبراني؟

أهمية الدراسة:

تتضح أهمية الدراسة في التالي:

- الأهمية العلمية:
 - يساهم البحث في زيادة المعرفة والفهم المتعمق لمفهوم إدارة مخاطر الأمن السيبراني وتشريعات الهيئة الوطنية للأمن السيبراني. ويمكن أن يوفر البحث نظرة شاملة حول الإطار القانوني والتنظيمي المعمول به وكيفية تطبيقه لإدارة مخاطر الأمن السيبراني للشركات.
 - يمكن أن يساهم البحث في تطوير النهج العلمي لإدارة مخاطر الأمن السيبراني. ومن خلال دراسة التشريعات المعمول بها وتحليلها، يمكن أن يتم تحديد الثغرات والتحديات في النهج الحالي واقتراح تحسينات وتوجهات جديدة لتعزيز الأمن السيبراني.
 - يمكن أن يكون البحث نقطة انطلاق للبحوث المستقبلية في مجال إدارة مخاطر الأمن السيبراني. وقد يشجع البحث العلماء والباحثين على استكشاف مواضيع ذات صلة وتطوير إطارات ونماذج جديدة لفهم ومعالجة التهديدات السيبرانية.
- الأهمية التطبيقية:
 - يمكن أن يساهم البحث في تحسين مستوى الأمن السيبراني في المؤسسات والمنظمات والهيئات. وعن طريق فهم تشريعات الهيئة الوطنية للأمن السيبراني وتطبيقها بشكل صحيح، يمكن للمؤسسات تعزيز قدراتها على اكتشاف واحتواء واستجابة التهديدات السيبرانية بشكل جيد.
 - يساعد البحث على فهم متطلبات الامتثال لتشريعات الهيئة الوطنية للأمن السيبراني. ويمكن للمؤسسات والشركات أن تستفيد من هذا البحث للامتثال بالتشريعات وتنفيذ إجراءات وسياسات تعزيز من مستوى الأمن السيبراني وتجنب المخاطر القانونية والعقوبات المحتملة.
 - يمكن أن يساهم البحث في تعزيز وعي الفرق العاملة وتعزيز قدراتها في إدارة مخاطر الأمن السيبراني. ومن خلال دراسة التشريعات وتحليلها، يمكن تطوير برامج تدريبية تستهدف توعية الموظفين وتعزيز مهاراتهم في التعامل مع التهديدات السيبرانية.
 - يمكن للبحث أن يساعد في توضيح المسؤوليات القانونية للشركات والأفراد فيما يتعلق بالأمن السيبراني. ومن خلال فهم تشريعات الهيئة الوطنية للأمن السيبراني وتطبيقها، يمكن للشركات تحديد مسؤولياتها واتخاذ الإجراءات اللازمة للحماية من التهديدات السيبرانية وتفادي المسائل القانونية.

أهداف الدراسة:

تهدف هذه الدراسة إلى التالي:

1. التعرف على إدارة مخاطر الأمن السيبراني في المملكة العربية السعودية.
2. التعرف على مدى الإلتزام بتشريعات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية.
3. التعرف على سبل تفعيل إدارة مخاطر السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني.

أسئلة الدراسة:

تتمثل مشكلة الدراسة في السؤال الرئيس التالي: التساؤل الرئيسي التالي: ماهي السبل المساعدة لإدارة مخاطر الأمن السيبراني في الشركات السعودية الخاصة بحسب تشريعات الهيئة الوطنية للأمن السيبراني؟ ويتفرع من التساؤل الرئيسي السابق التساؤلات الفرعية التالية:

1. ماهي مخاطر إدارة الأمن السيبراني في المملكة العربية السعودية؟
2. ما مدى الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية؟
3. ماهي السبل المساعدة لتفعيل إدارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني؟

الدراسات السابقة والاطار النظري:

أولاً: الدراسات السابقة تتناول الباحثة الدراسات السابقة مرتبة من الأقدم إلى الأحدث كما يلي:

- دراسة الصيدلاني (2017) بعنوان: واقع قرصنة البرمجيات في الأردن ، وسبل مواجهتها. وهدفت الدراسة إلى: التعرف على واقع قرصنة البرمجيات في الأردن ، وسبل مواجهتها. وتم تطبيق الدراسة على عينة مكونة من 120 من موظفي (11) شركة خدمية بمدينة عمان العاصمة، وقد استخدمت الدراسة المنهج الوصفي التحليلي ، و تمثلت أداة الدراسة في الإستبانة . وقد توصلت الدراسة إلى عدة نتائج أهمها : إنه في حين تقع مسؤولية توعية الطلبة بحقوق الملكية الفكرية ومخاطر القرصنة على قطاع التعليم فإن توعية عامة الشعب بمختلف مستوياتهم تقع على عاتق الحكومة والقطاع الخاص. والتأكيد بأن زيادة الوعي مفتاح القدرة على الحد من ظاهرة القرصنة.
- دراسة ستيفن Stephen (2017) بعنوان: أسباب توجه الأفراد والمنظمات إلى انتهاك خصوصية المعلومات ، ودور الأمن السيبراني في مواجهة الظاهرة. هدف البحث إلى التعرف على أسباب توجه الأفراد والمنظمات إلى انتهاك خصوصية المعلومات ودور الأمن السيبراني في مواجهة الظاهرة. وقد استخدم الباحث المنهج الوصفي المسحي وأداة الإستبانة وطبق دراسته على (124) من خبراء تكنولوجيا المعلومات بمؤسسة جون بريد بضاحية لندن الغربية بالمملكة المتحدة. وقد توصلت الدراسة إلى نتائج هامة، ومنها: تقديم اقتراح ببعض الحلول للحد من الظاهرة في المدارس مثل توعية الطلبة والمدرسين بالمسؤوليات والقيود الواجب مراعاتها عند استخدام البرمجيات، إضافة إلى جعل السياسات المتعلقة بقرصنة البرمجيات جزء من سياسات حقوق الطبع لفائدتها على الرغم من كلفتها العالية.
- دراسة والدو Waldo (2018) بعنوان: التوعية السيبرانية بخصوصية المعلومات والبيانات باستخدام الرحلات المعرفية عبر الويب ، مدخل تعليمي جديد في الاتحاد الأوروبي. هدفت الدراسة إلى توجيه نظر القائمين على السياسة الأمنية في الاتحاد الأوروبي إلى اعتماد استخدام الرحلات المعرفية عبر الويب ، كمدخل تعليمي جديد لاتخاذ القرارات بدلا من استخدامها بشكل فردي من قبل بعض المؤسسات . وقد عرف الباحث الرحلة المعرفية عبر الانترنت بأنها عبارة عن نشاط مبني على رحلة باستخدام الانترنت يتم عرضه مسبقاً، وتعليم الطلبة استخدام المعرفة المراد تعليمها للطلبة وكيفية التعامل معها. وقد استخدم الباحث المنهج المسحي وأداة الإستبانة . وقد طبق الباحث دراسته على (7) جامعات ومعاهد علمية في بلجيكا

وبريطانيا وهولندا . وقد توصلت الدراسة إلى نتائج هامة ومنها : أن إستراتيجية الرحلات المعرفية عبر الويب القائمة على محاكاة خصوصية البيانات تسهل على الجهات الأمنية التوعية بخصوصية المعلومات ومصادر المعرفة المتاحة ، على شبكة الإنترنت.

- دراسة الزهراني (2018) بعنوان: آثار قرصنة البرمجيات عالمياً. وتمثل هدف الدراسة في التعرف على آثار قرصنة البرمجيات عالمياً . وقد استخدمت الدراسة المنهج الوصفي التحليلي . وطبقت الدراسة على (79) من خبراء تكنولوجيا المعلومات بجامعة القاهرة . و تم استخدام الاستبانة في جمع البيانات . و من أهم نتائج الدراسة ما يلي : إن من أسباب انخفاض نسبة القرصنة في بعض الدول وجود حماية قوية للاختراعات والبرامج وحقوق الملكية الفكرية ، عكس الحال في كثير من الدول النامية .
- دراسة العضياني (2018) بعنوان: انتهاك خصوصية البيانات في مؤسسات الأعمال وأثره على أداء المؤسسات . وتمثلت أهداف الدراسة في التعرف على واقع انتهاك خصوصية البيانات في مؤسسات الأعمال وأثره على أداء المؤسسات. وقد استخدمت الدراسة المنهج الوصفي التحليلي . و بلغ حجم عينة الدراسة 132 من مدراء المؤسسات الخاصة وكبار الموظفين بها في مدينة القاهرة ، وتم جمع البيانات من خلال الاستبانة . و من أبرز النتائج التي توصل إليها الباحث ، ما يلي: إن اختراق أنظمة المعلومات و نظم الشبكات و المواقع المعلوماتية أصبح خطراً يقلق العديد من المنظمات ، إن هناك ارتفاعاً واضحاً في معدل الإختراقات مع تنوع الوسائل المستخدمة في الاختراق على الرغم من سبل الحماية التي تتبعها المنظمات.
- دراسة فايز (2019) بعنوان: دور تكنولوجيا المعلومات في تدعيم أداء الموارد البشرية (دراسة ميدانية). هدفت الدراسة إلى التعرف على دور تكنولوجيا المعلومات في تدعيم أداء الموارد البشرية بالشركات المصرية ، وقد استخدم الباحث المنهج الوصفي وأداة الإستبانة . وتمثلت عينة الدراسة في (118) من العاملين بشركة جهينة بمصر. وقد توصلت الدراسة إلى نتائج هامة ومنها: أن تكنولوجيا المعلومات تعمل على تطوير أداء الموارد البشرية بالشركة ، و أبدى أغلبية عينة الدراسة (98% منهم) شعورهم الإيجابي بأهمية التدريب.
- دراسة إبداع (2019) بعنوان: أمن وسرية المعلومات وأثرها على الأداء التنافسي دراسة تطبيقية في شركتي التأمين العراقية العامة والحمراء للتأمين الأهلية. وقد هدفت الدراسة إلى التعرف على أمن وسرية المعلومات وأثرها على الأداء التنافسي دراسة تطبيقية في شركتي التأمين العراقية العامة والحمراء للتأمين الأهلية. وطبقت هذه الدراسة في شركة التأمين العراقية العامة وشركة الحمراء للتأمين الأهلية نموذجاً عن شركات التأمين في العراق وباختبار عينة من المديرين والموظفين العاملين في الشركتين وبعدها (70) موظفاً، وقد استخدمت تلك البيانات في اختبار الفرضيات. وقد توصلت إلى الدراسة إلى عدد من الاستنتاجات كان أهمها وجود علاقة ارتباط وتأثير بين أمن المعلومات وسريتها والأداء التنافسي لشركات التأمين قيد البحث. وجاءت النتائج متطابقة مع فرضية الدراسة.
- دراسة ليبس Lipps (2020) بعنوان: الاهتمام بتنظيم دورات تكنولوجيا المعلومات ، مدخل تعليمي جديد في الاتحاد الأوروبي. وهدفت الدراسة إلى توجيه نظر القائمين على السياسة التعليمية في الاتحاد الأوروبي إلى الاهتمام بتنظيم دورات تكنولوجيا المعلومات كمدخل تعليمي جديد بدلا من استخدامها بشكل فردي من قبل المؤسسات بدول الاتحاد. وقد استخدم الباحث المنهج المسحي وأداة الإستبانة. وقد طبق الباحث

دراسته على (7) جامعات ومعاهد علمية في بلجيكا وبريطانيا وهولندا. وقد توصلت الدراسة إلى نتائج هامة ومنها : إن التقنيات الحديثة في تنمية الموارد البشرية تعتبر عصب الحياة العملية فهي ترفع من معنويات الفرد و تزيد فاعليته و ثقته، وتقلل من ضعفه النفسي أمام الآخرين ، إن استخدام المنظمات لنظم المعلومات ذات الكفاءة والفعالية من شأنه أن يحقق لها أهدافها.

- دراسة حمدان (2021) بعنوان: أمن وسرية المعلومات وأثرها في الأداء المصرفي: دراسة تطبيقية على البنوك العاملة في الأردن. هدفت هذه الدراسة إلى تعرف أمن المعلومات وسريتها وأثرها في الأداء المصرفي في البنوك العاملة في الأردن، وقد تكون مجتمع الدراسة من البنوك العاملة في الأردن، وأخذت عينة عشوائية طبقية متناسبة بنسبة 50% من مجتمع الدراسة (615) فرد. و أظهرت نتائج الدراسة أن مستوى ممارسة أمن المعلومات وسريتها في البنوك العاملة في الأردن من حيث الأهمية النسبية كانت مرتفعة، إذ بلغ المتوسط الحسابي (4.11). كما تبين أن الأهمية النسبية للأداء المصرفي في البنوك العاملة في الأردن كانت مرتفعة، إذ بلغ المتوسط الحسابي (4.07) وبينت نتائج الدراسة وجود أثر ذي دلالة إحصائية لأمن المعلومات وسريتها (الحماية المادية، حماية الأفراد، الحماية البرمجية) في الأداء المصرفي في البنوك العاملة في الأردن.
- دراسة ليرنر Lerner (2021) بعنوان: دور تكنولوجيا المعلومات في إعداد الكفاءات البشرية بمركز (ايزونتي). هدفت الدراسة إلى عرض تجربة مركز (ايزونتي للصحة النفسية) بمدينة (أنطويرب) ببلجيكا في إعداد الكفاءات البشرية. وطبقت الدراسة على عدد (26) من العاملين. وقد توصلت الدراسة إلى نتائج هامة ومنها : إن التخطيط المسبق لإعداد الموارد البشرية يساعد على تلافي السلبيات ، يمكن الاعتماد على تكنولوجيا المعلومات في إعداد الموارد البشرية نظرا لفاعليتها الكبيرة.

التعقيب على لدراسات السابقة:

بعد استعراض الدراسات السابقة تبين مايلي:

اتفقت الدراسة الحالية مع الدراسات السابقة في التركيز على موضوع الأمن السيبراني، كما اتفقت الدراسة الحالية مع بعض الدراسات السابقة في استخدام المنهج الوصفي. واختلفت الدراسة الحالية عن الدراسات السابقة لاختلاف الزوايا التي تم تناولها واختلاف الأهداف التي سعت إليها كل دراسة. كما تناولت الدراسات السابقة موضوع الدراسة في بيانات مختلفة عن بيئة الدراسة الحالية بالإضافة إلى اختلاف الفترة الزمنية التي سوف تتم فيها الدراسة الحالية عن الفترات الزمنية التي تمت في الدراسات السابقة. كما أنه سيتم الاستفادة من الدراسات السابقة بالتالي:

- التأصيل النظري للدراسة الحالية.
- تحديد مصطلحات الدراسة.
- الاطلاع على دراسات سابقة في موضوع الدراسة الحالية
- الاستفادة من الدراسات السابقة في تحديد منهج الدراسة
- بناء أداة الدراسة
- تحديد الأساليب الاحصائية المناسبة

المنطلقات النظرية للدراسة:

تتمثل النظريات المفسرة لإدارة مخاطر الأمن السيبراني، فيما يلي:

1. نظرية النموذج الدائري للأمن السيبراني (Cybersecurity Diamond Model): تعتبر هذه النظرية منهجاً شاملاً لفهم وتحليل الأمن السيبراني. وتتألف النظرية من أربع عناصر رئيسية هي: المهاجم (Adversary)، والضحية (Victim)، والسلوك (Behavior)، والتهديدات والضعف (Threats and Weaknesses). وتعزز هذه النظرية فهم كيفية تفاعل هذه العناصر وتوفر إطاراً لتحليل المخاطر وتصميم استراتيجيات الحماية.
2. نظرية الانحدار العُقدي للأمن السيبراني (Cybersecurity Maturity Model): تركز هذه النظرية على تقييم مستوى نضج أمان المؤسسة أو المنظمة. وتعتمد النظرية على تقدير القدرة على التحمل والاستجابة والاستعادة بعد وقوع الهجمات السيبرانية، كما تساعد هذه النظرية المؤسسات على تحديد نقاط الضعف وتحسين قدراتها في مجال الأمن السيبراني.
3. نظرية السلسلة الإمدادية للأمن السيبراني (Cybersecurity Supply Chain): تركز هذه النظرية على أهمية حماية سلاسل الامداد التكنولوجي والتأكد من أمان الموردين والجهات الفاعلة الأخرى في البيئة السيبرانية. وتعتبر هذه النظرية مهمة في تقييم المخاطر المحتملة التي يمكن ان تنشأ عند التعامل مع جهات خارجية (فايز، 2019، ص 45-47).
4. نظرية السلوك البشري في الأمن السيبراني (Human Behavior in Cybersecurity): تركز هذه النظرية على الجانب البشري في أمن المعلومات والأمن السيبراني. وتهدف النظرية إلى فهم سلوك المستخدمين والعاملين في المؤسسات وكيفية تأثيرهم على مخاطر الأمن السيبراني. وتعتبر التوعية والتدريب السلوكي للمستخدمين جزءاً أساسياً من هذه النظرية.
5. نظرية النموذج العام للتهديدات السيبرانية (General Model of Cyber Threats): تقدم هذه النظرية نموذجاً شاملاً لفهم التهديدات السيبرانية وأنماطها. وتعتمد النظرية على تحليل الهجمات السيبرانية السابقة والتعرف على الأنماط المشتركة والعوامل المؤثرة في تكرارها. ويتيح هذا النموذج تحديد الثغرات الأمنية المحتملة واتخاذ التدابير الوقائية المناسبة.
6. نظرية تحليل الأخطار (Risk Analysis Theory): تركز هذه النظرية على تحليل المخاطر وتقييمها في سياق الأمن السيبراني. وتعتمد النظرية على تحديد وتصنيف المخاطر السيبرانية المحتملة وتقييم مدى تأثيرها واحتمالية حدوثها. ويتيح هذا التحليل للمؤسسات تحديد الأولويات وتخصيص الموارد للتعامل مع المخاطر الأكثر تأثيراً.
7. نظرية الاستجابة للحوادث السيبرانية (Incident Response Theory): تهدف هذه النظرية إلى تطوير إطار عمل للاستجابة الفعالة للحوادث السيبرانية. وتشمل هذه النظرية إجراءات وممارسات للكشف عن الاختراقات والتعامل معها واستعادة النظام بعد الحادث. وتوفر هذه النظرية الارشادات اللازمة للمؤسسات للتعامل مع الحوادث السيبرانية بشكل منهجي وفعال.

المنهجية وطرق البحث:

- منهج الدراسة:
تتبع الباحثة في هذه الدراسة المنهج الوصفي التحليلي، إذ يختص بوصف الواقع من أجل فهمه وكيفية التعامل معه فهو تمهيد منطقي لوصف واقع الحال.
- مجتمع وعينة البحث:
سوف يتحدد مجتمع الدراسة في بعض من منسوبي المؤسسات التكنولوجية في منطقة الرياض والبالغ عددهم (840) موظف وموظفة (الهيئة العامة للإحصاء، 1443، ص96). حيث سيتم اختيار نسبة لا تقل عن 30% من منسوبي المؤسسات التكنولوجية في منطقة الرياض. وسوف يتم اختيار العينة بالطريقة العشوائية عن طريق وضع الأسماء على جهاز الحاسب الآلي والاختيار بينها. كما ستكون هذه الدراسة من التالي:

- الفصل الأول: مقدمة البحث
- الفصل الثاني: الاطار النظري والدراسات السابقة
- الفصل الثالث: اجراءات البحث (المنهجية والاجراءات)
- الفصل الرابع: الدراسة الميدانية وتحليل ومناقشة النتائج
- الفصل الخامس: خلاصة لأهم نتائج الدراسة وتوصياتها
- المصادر والمراجع، ثم الملاحق

أدوات البحث (أدوات جمع البيانات):

ستقوم الباحثة بتصميم استبانة من خلال النظر إلى الأدبيات والدراسات السابقة، وسوف تتكون أداة الدراسة من قسمين موضحة فيما يلي:

- القسم الأول: البيانات الشخصية، ويشمل على ثلاثة أبعاد رئيسية وهي:
 - المؤهل العلمي
 - عدد سنوات الخبرة
 - عدد الدورات التدريبية
- القسم الثاني: محاور الاستبانة، ويشمل على ثلاث أبعاد رئيسية وهي:
 - المحور الأول: مخاطر الأمن السيبراني في المملكة العربية السعودية
 - المحور الثاني: مدى الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني
 - المحور الثالث: سبل مساعدة لتفعيل ادارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني

كما أنه سيتم استخدام مقياس ليكرت الخماسي في البحث للتعرف على استجابات عينة الدراسة لفقرات الاستبانة، والجدول التالي يوضح بدائب الاستجابات:

جدول رقم (1)

مقياس ليكرت الخماسي

المعيار	موافق بشدة	موافق	إلى حد ما	غير موافق	غير موافق بشدة
الدرجة	5	4	3	2	1
المتوسط الحسابي	5.00-4.20	4.19-3.40	3.39-2.60	2.59-1.80	1.79-1.00
درجة الموافقة	مرتفعة جداً	مرتفعة	متوسطة	منخفضة	منخفضة جداً

مجالات الدراسة (بشري، مكاني، زمني):

تحدد الدراسة الحالية بالحدود التالية:

- الحدود الموضوعية:
تركز الدراسة الحالية على ادارة مخاطر الأمن السيبراني بحسب تشريعات الهيئة الوطنية للأمن السيبراني.
- الحدود البشرية:
منسوبي المؤسسات التكنولوجية
- الحدود المكانية:
منطقة شرق الرياض
- الحدود الزمنية:
سوف تجري الدراسة خلال العام 1445هـ / 2023م.

الفصل الثاني

1- مفهوم الأمن السيبراني:

الأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به و سوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني. كما يعد الأمن السيبراني سلاح استراتيجي بيد الحكومات والإفراد لا سيما أن الحرب السيبرانية أصبحت جزءاً لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول. وينتهج الأمن السيبراني الناجح نهجاً يتكون عادةً من طبقات متعددة للحماية تنتشر في أجهزة الكمبيوتر أو الشبكات أو البرامج أو البيانات التي ينوي المرء الحفاظ على سلامتها، ففي أي منظمة يجب على المستخدمين والعمليات والتكنولوجيا أن يكملوا بعضهم بعضاً ويتكاتفوا لإنشاء دفاع فعال من الهجمات السيبرانية. وفي عصر التكنولوجيا أصبح لأمن المعلومات الدور الأكبر صد ومنع أي هجوم إلكتروني قد تتعرض له أنظمة الدولة المختلفة، وأيضا حماية الأنظمة التشغيلية من محاولات الولوج بشكل غير مسموح به لأهداف غير سليمة، وهو السبب وراء الأمر الملكي بإنشاء الهيئة الوطنية للأمن السيبراني (الشراري ، 2017، ص39-40).

إن هدف الأمن السيبراني هو المساعدة على حماية أصول المنظمات ومواردها من النواحي التنظيمية، والبشرية، والمالية، والتقنية والمعلوماتية بحيث يسمح لها بمواصلة مهمتها. والهدف النهائي هو ضمان عدم تضررها بشكل جسيم ودائم. وهذا يتمثل في تقليل احتمالات تجسد أي تهديد، والحد من الضرر الناجم أو سوء الأداء، وضمان استعادة العمليات لحالتها السابقة خلال إطار زمني محدد وبتكلفة مقبولة في أعقاب وقوع حوادث الأمن السيبراني. وتشمل عملية الأمن السيبراني المجتمع بأسره، من حيث يكون كل فرد فيه معنياً بتنفيذها. ويمكن دعم ذلك بتطوير مدونة سلوك سيبرانية لأجل الاستخدام السليم لتكنولوجيا المعلومات والاتصالات، وإعلان سياسات أمن واقعية تقنن المعايير التي يكون متوقعاً من مستخدمي الأمن السيبراني (الكيانات والشركاء والموردون) الوفاء بها. ولإنشاء عملية أمن سيبراني، يكون من المهم التحديد الدقيق للأصول والموارد اللازمة للوقاية الفعالة. ويستلزم ذلك نهجاً عالمياً للأمن، نهجاً متعدد التخصصات وشاملاً إذ لا يصلح الأمن السيبراني في عالم يسوده التسبب ويعتقن الإباحية. والمطلوب هو مجموعة من المبادئ الأساسية للسلوك الأخلاقي، والمسؤولية والشفافية المتجسدة في إطار قانوني مناسب، ومجموعة عملية من الإجراءات والقواعد. ويجب إنفاذ تلك المبادئ محلياً، بالطبع، ولكن ينبغي أيضاً تطبيقها عبر المجتمع الدولي وأن تكون متوافقة مع التوجهات الدولية القائمة. ولتفادي إتاحة الفرص أمام تنامي الجريمة، يجب على البنى التحتية للاتصالات أن تشتمل على تدابير أمن مناسبة ذات طبيعة تقنية وقانونية مناسبة. ويمكن للهجمات عبر الفضاء السيبراني أن تتخذ أشكالاً كثيرة: الاختطاف السري لنظام، رفض تقديم الخدمة، تدمير أو سرقة بيانات حساسة، اقتحام المتسللين للشبكة، كسْر حماية البرمجيات، الفركنة أو التنصت الإلكتروني (phreaking) والذي يشمل التخريب واختطاف المبادلات الهاتفية وأكثر من ذلك. وتقع تكلفة ذلك في الغالب الأعم على عاتق الضحايا، أي المنظمات والأفراد المستهدفين (الاتحاد الدولي للاتصالات، 2019، ص11-13).

2- أهمية الأمن السيبراني:

تحدد أهداف الأمن السيبراني فيما يلي:

1- الحماية من الهجمات السيبرانية:

يتعرض الأفراد والشركات والمؤسسات والحكومات للعديد من التهديدات السيبرانية مثل اختراق الأنظمة، والبرمجيات الخبيثة، والاحتيايل الإلكتروني، وتسريب المعلومات الحساسة، والإرهاب الإلكتروني، والتجسس السيبراني. ويهدف الأمن السيبراني إلى توفير الحماية اللازمة للأنظمة والبيانات والمعلومات ضد هذه الهجمات.

2- الحفاظ على الخصوصية:

تعتبر الخصوصية أحد جوانب الأمن السيبراني المهمة. ويجب حماية البيانات الشخصية والمعلومات الحساسة للأفراد والمؤسسات من الوصول غير المصرح به والاستخدام غير القانوني. فقد تتضمن هذه المعلومات المالية، والطبية، والتجارية، والحكومية، والخاصة. يتطلب الأمر تنفيذ إجراءات الحماية المناسبة مثل تشفير البيانات وضمان الوصول المحدود للأشخاص المخولين فقط.

3- الحفاظ على استقرار الأنظمة:

يعتمد العديد من الجوانب في حياتنا اليومية على الأنظمة السيبرانية مثل النظام المصرفي والشبكات الاجتماعية والنقل العام والتجارة الإلكترونية. ويهدف الأمن السيبراني إلى ضمان استقرار هذه الأنظمة ومنع تعطيلها أو تعرضها للهجمات التي يمكن أن تتسبب في فوضى وتوقف الخدمات الحيوية (الزهراني، 2018، ص 47-49).

4- الحماية الوطنية والاقتصادية:

يعد الأمن السيبراني أحد جوانب الأمن الوطني، حيث يمكن للهجمات السيبرانية المستهدفة للبنى التحتية الحيوية للدولة أن تسبب أضراراً جسيمة على المستوى الاقتصادي والعسكري والسياسي. وتستهدف بعض الهجمات السيبرانية الحكومات والمؤسسات الحكومية والبنى التحتية الحيوية مثل الشبكات الكهربائية والمياه والمواصلات. ويعمل الأمن السيبراني على تعزيز القدرة التنافسية للدول والاقتصادات من خلال حماية المعلومات الاقتصادية والتكنولوجية الحساسة ومنع سرقتها أو تسريبها.

5- الحماية من التجسس الصناعي:

تعاني العديد من الشركات من التجسس الصناعي الذي يستهدف سرقة المعلومات التجارية والتكنولوجية الحساسة. ويتطلب الأمن السيبراني تنفيذ إجراءات لحماية الملكية الفكرية والأسرار التجارية وضمان عدم الوصول غير المصرح به إلى هذه المعلومات.

6- الحماية الشخصية:

يعتبر الأمن السيبراني أيضاً أمراً هاماً للأفراد. ويجب على الأفراد اتخاذ إجراءات الأمان السيبراني لحماية هويتهم الشخصية والمعلومات الشخصية الحساسة مثل المعلومات المالية والصحية والخصوصية الشخصية على الإنترنت. ويشمل ذلك استخدام كلمات مرور قوية، وتحديث برامج الحماية (الصيدلاني، 2017، ص 95-97).

3- أهداف الأمن السيبراني:

تتحدد أهداف الأمن السيبراني فيما يلي:

- 1- حماية السرية والخصوصية: يهدف الأمن السيبراني إلى حماية البيانات والمعلومات الحساسة من الوصول غير المصرح به والاستخدام غير القانوني. ويتم تنفيذ تدابير الأمان مثل التشفير وإدارة الوصول للحفاظ على سرية المعلومات وحماية خصوصية الأفراد والمؤسسات.
- 2- ضمان توافر الأنظمة: يهدف الأمن السيبراني إلى ضمان توافر الأنظمة والخدمات السيبرانية المهمة. ويتضمن ذلك حماية الأنظمة من الهجمات السيبرانية المتعمدة التي تهدف إلى تعطيلها أو إلحاق أضرار بها. ويتم تطبيق تدابير الأمان مثل إعدادات الحماية والنسخ الاحتياطي والاستعداد للكوارث لضمان استمرارية العمليات.
- 3- الوقاية من الهجمات السيبرانية: يشمل الهدف الأساسي للأمن السيبراني الوقاية من الهجمات السيبرانية المحتملة. ويتم تحليل ومراقبة الأنشطة السيبرانية لاكتشاف التهديدات المحتملة والاستجابة لها قبل حدوث الأضرار. ويشمل ذلك استخدام أدوات الكشف عن التسلل وأنظمة الإنذار المبكر والتحليل الأمني للكشف عن الهجمات والتصدي لها.
- 4- تعزيز الاستعداد والاستجابة: يهدف الأمن السيبراني إلى تعزيز الاستعداد والاستجابة للهجمات السيبرانية. ويتضمن ذلك وضع خطط الطوارئ والاستجابة للتعامل مع الهجمات واحتواء الأضرار واستعادة النظم إلى حالتها الطبيعية بأقل وقت ممكن. كما يشمل تقييم التهديدات وتحديث السياسات والإجراءات لمواجهة التهديدات المتغيرة.
- 5- تعزيز التوعية والتدريب: يهدف الأمن السيبراني إلى تعزيز التوعية والتدريب للأفراد والمؤسسات بشأن التهديدات السيبرانية وأفضل الممارسات للوقاية منها. ويهدف ذلك إلى زيادة الوعي بأمن المعلومات وتعزيز المهارات الفنية لتأمين الأنظمة والشبكات السيبرانية تتطلب تنفيذ استراتيجيات وتدابير أمنية متعددة لتحقيق هذه الأهداف. ويجب أن تكون هذه التدابير شاملة وتشمل الجوانب التقنية والتنظيمية والتعليمية والقانونية (فايز، 2019، ص 63-65).

4- العناصر الأساسية للأمن السيبراني:

تتحدد العناصر الأساسية للأمن السيبراني ، فيما يلي :

- 1- منظومة الأجهزة الإلكترونية وملحقاتها: إن أجهزة الحواسيب تتطور بشكل هائل بالمقابل هناك تطور في مجال السبل المستخدمة لاختراقها مما يتطلب تطوير القابليات و المهارات للعاملين في أقسام المعلومات لكي يستطيعوا مواجهة حالات التلاعب و العبث المقصود في الأجهزة أو غير المقصود .
- 2- الأفراد العاملين في أقسام المعلومات: يلعب الفرد دوراً أساسياً ومهماً في مجال أمن المعلومات و الحواسيب و له تأثير فعال في أداء عمل الحواسيب بجانبه الإيجابي و السلبي ، فهو عامل مؤثر في حماية الحواسيب و المعلومات و لكن في الوقت نفسه فإنه عامل سلبي في مجال تخريب الأجهزة و سرقة المعلومات سواء لمصالح ذاتية أو لمصالح الغير ، إن من متطلبات أمن الحواسيب تحديد مواصفات محددة للعاملين و وضع تعليمات واضحة لاختيارهم و ذلك للتقليل من المخاطر التي يمكن أن يكون مصدرها الأفراد إضافة الى وضع الخطط

لزيادة الحس الأمني و الحصانة من التخريب ، كما يتطلب الأمر المراجعة الدورية للتدقيق في الشخصية والسلوكية للأفراد العاملين من وقت لآخر و ربما يتم تغيير مواقع عملهم و محاولة عدم احتكار المهام على موظفين محددين (سكيكر ، 2010 ، ص 49-51).

3- البرمجيات المستخدمة في تشغيل النظام: تعتبر البرمجيات من المكونات غير المادية و عنصر أساس في نجاح استخدام النظام ، لذلك من الأفضل اختيار حواسيب ذات أنظمة تشغيل لها خصائص أمنية و يمكن أن تحقق حماية للبرامج و طرق حفظ كلمات السر و طريقة إدارة نظام التشغيل و أنظمة الاتصالات، إن أمن البرمجيات يتطلب أن يؤخذ هذا الأمر بعين الاعتبار عند تصميم النظام و كتابة برامجه من خلال وضع عدد من الإجراءات كالمفاتيح والعوائق التي تضمن عدم تمكن المستفيد من التصرف خارج الحدود المخول بها و تمنع أي شخص من إمكانية التلاعب و الدخول إلى النظام و ذلك من خلال أيضا تحديد الصلاحيات في مجال قراءة الملفات أو الكتابة فيها ، و محاولة التمييز بين اللذين يحق لهم الإطلاع و حسب كلمات السر الموضوعة ، وهناك أسلوبان للتمييز إما عن طريق البرمجيات أو استخدام الأجهزة المناسبة (السالمي ، 2019 ، ص 125-127).

4- شبكة تناقل المعلومات: تعتبر شبكة تناقل المعلومات المحلية أو الدولية ثمرة من ثمرات التطورات في مجالات الاتصالات كما أنها سهلت عملية التراسل بين الحواسيب و تبادل و استخدام الملفات ، و لكن من جهة أخرى إتاحة عملية سرقة المعلومات أو تدميرها سواء من الداخل كاستخدام الفيروسات أو من خلال الدخول عبر منظومات الاتصال المختلفة ، لذلك لا بد من وضع إجراءات حماية و ضمان أمن الشبكات من خلال إجراء الفحوصات المستمرة لهذه المنظومات و توفير الأجهزة الخاصة بالفحص ، كما أن نظم التشغيل المستخدمة و المسئولة عن إدارة الحواسيب يجب أن تتمتع بكفاءة و قدرة عالية على الكشف عن التسلل إلى الشبكة و ذلك من خلال تصميم نظم محمية بإقفال معقد أو عن طريق المجفترات و ربطها بخطوط الاتصال و التي هي عبارة عن استخدام الخوارزميات الرياضية أو أجهزة و معدات لغرض تجفير تناقل المعلومات (عبد ربه ، 2013 ، ص 60-61).

5- مواقع منظومة الأجهزة الإلكترونية وملحقاتها: يجب أن تعطى أهمية للمواقع و الأبنية التي يحوي أجهزة الحواسيب و ملحقاتها ، و حسب طبيعة المنظومات و التطبيقات المستخدمة يتم اتخاذ الإجراءات الاحترازية لحماية الموقع و تحصينه من أي تخريب أو سطو و حمايته من الحريق أو تسرب المياه و الفيضانات ، و محاولة إدامة مصدر القدرة الكهربائية و انتظامها و تحديد أساليب و إجراءات التفتيش و التحقق من هوية الأفراد الداخلين و الخارجين من الموقع و عمل سجل لذلك (السالمي ، 2019 ، ص 133).

6- شبكة تناقل المعلومات: تعتبر شبكة تناقل المعلومات المحلية أو الدولية ثمرة من ثمرات التطورات في مجالات الاتصالات كما أنها سهلت عملية التراسل بين الحواسيب و تبادل و استخدام الملفات ، و لكن من جهة أخرى إتاحة عملية سرقة المعلومات أو تدميرها سواء من الداخل كاستخدام الفيروسات أو من خلال الدخول عبر منظومات الاتصال المختلفة ، لذلك لا بد من وضع إجراءات حماية و ضمان أمن الشبكات من خلال إجراء الفحوصات المستمرة لهذه المنظومات و توفير الأجهزة الخاصة بالفحص ، كما أن نظم التشغيل المستخدمة و المسئولة عن إدارة الحواسيب يجب أن تتمتع بكفاءة و قدرة عالية على الكشف عن التسلل إلى الشبكة و ذلك من خلال تصميم نظم محمية بإقفال معقد أو عن طريق المجفترات و ربطها

بخطوط الاتصال و التي هي عبارة عن استخدام الخوارزميات الرياضية أو أجهزة و معدات لغرض تجفير
تناقل المعلومات (عبد ربه ، 2013 ، ص60-61).

7- مواقع منظومة الأجهزة الإلكترونية وملحقاتها: يجب أن تعطى أهمية للمواقع و الأبنية التي يحوي أجهزة
الحواسيب و ملحقاتها ، و حسب طبيعة المنظومات و التطبيقات المستخدمة يتم اتخاذ الإجراءات الإحترازية
لحماية الموقع و تحصينه من أي تخريب أو سطو و حمايته من الحريق أو تسرب المياه و الفيضانات ، و
محاولة إدامة مصدر القدرة الكهربائية و انتظامها و تحديد أساليب و إجراءات التفتيش و التحقق من
هوية الأفراد الداخلين و الخارجين من الموقع و عمل سجل لذلك (السالمي ، 2019 ، ص133).

إن ثورة المعلومات تحدث تغييرات عميقة في الطريقة التي تتم بها معالجة المعلومات وتخزينها. وهي تغير الطريقة التي
تؤدي بها المنظمات، بل المجتمع ككل في حقيقة الأمر، وظائفه. فهي ليست الابتكار التقني الوحيد الذي حدث خلال
السنوات الأخيرة، وإنما تبرز بسبب تأثيرها على معالجة المعلومات، ومن ثم على المعارف. ولأن ثورة المعلومات تؤثر في
الآليات التي تُخلَق بها المعارف وبها يتم تقاسمها، فيمكن اعتبارها منبعاً للابتكار في المستقبل لا ينبغي استبعاد البلدان
النامية عنه. فتورة المعلومات وتكنولوجيات الاتصالات تؤدي إلى ثورة حقيقية في كيفية تفكيرنا في المبادلات
الاقتصادية والاجتماعية والثقافية. وهي تزودنا كذلك بنموذج جديد لتكنولوجيا المعلومات يستند إلى الشبكة التي
يحتاج أمن انسياب المعلومات عبرها إلى تأمين حتى يمكن تطوير الاستخدامات التطبيقية الجديدة التي ستزيد من
فعالية التنظيمات. إذ لا يمكن لأي شكل من أشكال النشاط الاقتصادي أن يبقى بدون المبادلات وبدون التفاعل بين
المشاركين فيه، ولا يمكن أن يحدث أي تبادل للمعلومات دون وجود نوع من ضمانات الأمن الأساسية. ولا يمكن
تخطيط أي خدمة بدون مراعاة نوعية تلك الخدمة. غير أنه يجب علينا، مع ذلك، أن نضع نصب أعيننا أن نجاح
اتصال ما يعتمد على قدرة الأطراف الضالعة فيه على التعامل مع العقبات التقنية وإدارة العادات التي تدخل في أي
مبادلة للمعلومات (الهيئة الوطنية للأمن السيبراني، 2018، ص25-27).

5- عوامل تحقيق الأمن السيبراني:

هناك ثلاثة عوامل أساسية لتحقيق الأمن السيبراني وهي:

1- السرية Confidentiality:

وهي ضمان عدم تسريب أي معلومة من النظام إلى غير المصرح لهم بها.

2- الموثوقية Integrity:

وهو ضمان صحة المعلومات داخل النظام وسلامتها من التلاعب والتبديل والتعديل غير المصرح به.

3- التوافر Availability:

وهو ضمان سلامة النظام وقدرته على العمل وتوفير الخدمة/المعلومة إلى الأشخاص المصرح لهم وذوي

العلاقة، يعني ضمان عدم تعطل النظام بسبب هجمات إلكترونية أو ما شابه.

إن تحول المجتمعات إلى مجتمعات معلوماتية، وهو التحول الذي يحدث بفضل إدماج تكنولوجيات جديدة في كل
مجال من مجالات النشاط، وفي كل نوع من أنواع البنية التحتية ليزيد من اعتماد الأفراد، والمنظمات، والبلدان على
أنظمة المعلومات والشبكات. وهذا مصدر رئيسي من مصادر المخاطر تجب معاملته كخطر أمني. وتواجه البلدان
النامية إشكالية الحاجة للانضمام إلى المجتمع المعلوماتي دون أن يغيب عن بالها مخاطر تحولها إلى الاعتماد على

التكنولوجيات وعلى مقدمي التكنولوجيا واحتياجها لتفادي خطر الفجوة الرقمية التي تنشأ عنها ثغرة أمنية أو حتى الاعتماد الزائد على الهيئات التي تتحكم في احتياجاتها وفي سبل تحقيق أمن تكنولوجيا المعلومات. ويجب أن يتم التفكير ملياً في تصميم وإنشاء وإدارة البنى الأساسية للاتصالات والخدمات والأنشطة التي توفرها مع مراعاة الجانب الأمني، ذلك لأن الأمن هو الركن الركين لأي نشاط، وينبغي النظر إليه كخدمة تُمكن من خلق خدمات أخرى وتولد القيمة (مثل الحكومة الإلكترونية، والصحة الإلكترونية، والتعليم الإلكتروني). فليس الأمر مقصوراً على التكنولوجيا وحدها، ومع ذلك فإن أدوات الاتصال الأساسية المتوافرة حتى الآن لا تظفر بالموارد الضرورية والكافية لتوفير أو لضمان القدر الأدنى لها من الأمن (البار، 2021، ص13-15).

إن أنظمة تكنولوجيا المعلومات المترابطة شبكياً هي موارد يمكن الوصول إليها عن بعد، ومن ثم فهي أهداف يحتمل أن تتعرض للهجوم السيبراني. كما أن الأنظمة معرضة لخطر زائد هو الاختراق، حيث تزايد فرص شن الهجمات عليها واقتراف الجرائم. وعلى الرغم من أن الأنظمة هي التي تكون هدفاً للهجوم فإن الغنيمة التي يسعى المهاجمون للفوز بها هي المعلومات التي تجري معالجتها ويمكن لهذه الهجمات أن تنال من القدرة على المعالجة والتخزين وتقاسم الرصيد المعلوماتي، بل ويمكن لها أن تُنزل الضرر بالسلع غير الملموسة والرمزية، وبعمليات الإنتاج، وبعمليات صنع القرار لدى المنظمة. وتحمل الأنظمة السيبرانية المخاطر التشغيلية إلى المنظمات التي تمتلكها. وهكذا يمكن للتعامل مع مشاكل الأمن السيبراني المعقدة والمتعددة الأوجه أن يكون صعباً نسبياً، كما يمكن لمضاعفاتها المحتملة وتأثيراتها على تشغيل المنظمات والبلدان أن تكون مدمرة. وقد تتوقف العوامل المهمة للغاية لإنجاح الاقتصادات على قدرة توفير الأمن للمعلومات وللعمليات وللأنظمة وللبنية التحتية (الهيئة الوطنية للأمن السيبراني، 2018، ص19-20).

6- مخاطر الأمن السيبراني:

إن غرض الأمن السيبراني هو المساعدة على حماية أصول وموارد منظمة ما من النواحي التنظيمية، والبشرية، والمالية والتقنية والمعلوماتية بحيث تتمكن من أداء المهمة الموكلة إليها. والهدف الأسى لذلك هو ضمان عدم حدوث ضرر دائم للمنظمة. ويتألف ذلك من تقليل احتمالات تجسد خطرٍ ما، والحد من الضرر أو سوء الأداء الناجمين، وتأمين عودة العمليات العادية إلى مسيرتها الأولى بعد وقوع حادث أمني، خلال فترة زمنية مقبولة وبتكلفة ومعقولة. وتشمل عملية الأمن السيبراني المجتمع بأسره، بحيث يكون كل فرد مهتم بتنفيذه. ويمكن جعل هذه العملية أكثر أهمية عن طريق بلورة مدونة سلوك سيبراني، والإعلان عن سياسات أمن حقيقية تنص على المعايير التي يكون من المتوقع وفاء المستعملين، وكذلك الكيانات والشركاء والموردين بها. وتتعدد طبيعة الأخطار التي يمكن أن تواجهها نظم المعلومات فهي عديدة، فالبعض منها قد يكون مقصود كسرقة المعلومات أو إدخال الفيروسات وغيرها وهي الأشد ضرراً على نظم المعلومات ويكون مصدرها أحياناً من داخل أو خارج المنظمة، وقد يصعب أحياناً التنبؤ بالدوافع العديدة للأشخاص الذين يقومون بها، أما البعض الآخر فقد يكون غير مقصود كالأخطاء البشرية والكوارث الطبيعية (الغامدي، 2021، ص103-105).

ويمكن تصنيف الأخطار المحتملة التي يمكن أن تتعرض لها نظم المعلومات إلى ثلاث فئات رئيسية، وهي:

- 1- **الأخطاء البشرية:** وهي التي يمكن أن تحدث أثناء تصميم التجهيزات أو نظم المعلومات أو خلال عمليات البرمجة أو الاختبار أو التجميع للبيانات أو أثناء إدخالها إلى النظام، أو في عمليات تحديد الصلاحيات

للمستخدمين ، وتشكل هذه الأخطاء الغالبية العظمى للمشاكل المتعلقة بأمن و سلامة نظم المعلومات في المنظمات (القحطاني ، 2019 ، ص29).

2- المخاطر البيئية: وهي التي تشمل الزلازل و العواصف و الفيضانات و الأعاصير و المشاكل المتعلقة بأعطال التيار الكهربائي و الحرائق إضافة إلى المشاكل القائمة في تعطل أنظمة التكييف و التبريد و غيرها ، و تؤدي هذه الأخطار إلى تعطل عمل هذه التجهيزات و توقفها لفترات طويلة نسبياً لإجراء الإصلاحات اللازمة و استرداد البرمجيات و قواعد البيانات (ياغي ، 2017 ، ص32).

3- الجرائم الالكترونية: تمثل الجرائم الإلكترونية تحدياً كبيراً لإدارة نظم المعلومات لما تسببه من خسارة كبيرة للأشخاص وللمنظمات وللدول بشكل عام و للجريمة الالكترونية أنواع وهي:

- 1- الجريمة المادية، وهي التي تسبب أضرار على المستهدف مثل:
 - عملية الاحتيال الالكتروني كالسطو على ماكينات الصرف الآلي والبنوك.
 - جرائم التصيد كإنشاء صفحة انترنت مشابهة تماماً لموقع أحد البنوك الكبرى تتضمن رسالة احتيالية تطلب من المستخدم تحديث بيانات العملاء لفترة زمنية محددة وإلا تعرضت حساباتهم للإلغاء.
 - رسائل البريد الخادعة مثل التي تتضمن عرضاً بتحويل عدة ملايين إلى حساب الضحية لدى أحد البنوك مقابل نسبة منه ويطلب من الضحية إرسال مبلغ معين كزعم أنها رسوم إجراءات التحويل (ياغي ، 2017 ، ص36-37).

2- الجريمة الثقافية: وهي جرائم تتعلق بحقوق الملكية الفكرية لبرامج الكمبيوتر وكذلك سرقة بعض المعلومات المهمة والأفكار من أجهزة الضحايا ونسبها إليهم (ياغي ، 2017 ، ص47).

3- الجريمة السياسية والاقتصادية: وتتضمن التالي:

- نشر وإصدار إشاعات على مواقع ومراكز مهمة لكي تعطل مصالح الشعب.
- نشر السلوك الخاطئ كالإرهاب وإدمان الخمور والمخدرات حتى يفسدون المجتمع والشباب وذلك ليضرروا الدولة لأسباب سياسية واقتصادية (السالمي ، 2019 ، ص52-54).

4- الجريمة الجنسية: وتتضمن التالي:

- التغيرير والاستدراج وهي منتشرة بين أوساط صغار السن والمراهقين.
- سرقة المعلومات والصور والبيانات المتصلة بالحياة الخاصة والمساومة بها.
- نشر الصور ومقاطع الفيديو الإباحية بين الشباب والمراهقين (القحطاني ، 2019 ، ص58).

7- أهمية تشريعات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية:

تتحدد أهمية تشريعات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية في التالي:

1- حماية البنية التحتية الحيوية:

تساعد تشريعات الهيئة الوطنية للأمن السيبراني في حماية البنية التحتية الحيوية في المملكة العربية السعودية. وتعد هذه التشريعات الإطار القانوني الذي ينظم تصميم وتشغيل وصيانة الأنظمة السيبرانية

الحيوية مثل الأنظمة الحكومية والبنوك والشركات الحيوية الأخرى. وبالتالي، فإنها تحمي البنية التحتية الحيوية التي تعتبر حاسمة لاستمرارية العمليات الحكومية والاقتصادية والاجتماعية في البلاد.

2- مكافحة التهديدات السيبرانية:

تلعب تشريعات الهيئة الوطنية للأمن السيبراني دوراً هاماً في مكافحة التهديدات السيبرانية. وتوفر هذه التشريعات الأدوات القانونية اللازمة لمكافحة الهجمات السيبرانية وتتبع المهاجمين وتقديم العقوبات المناسبة لهم. بوجود هذا الإطار القانوني، تكون هناك رسالة قوية بأن التهديدات السيبرانية لا تسمح بها، وهذا يعزز ردع المهاجمين المحتملين ويحد من حدوث الهجمات.

3- تعزيز التعاون والتنسيق:

تشجع تشريعات الهيئة الوطنية للأمن السيبراني على التعاون والتنسيق بين الجهات المعنية في المملكة العربية السعودية. ويشمل ذلك التعاون بين القطاع العام والقطاع الخاص والمؤسسات الأكاديمية والمجتمع المدني. بواسطة هذه التشريعات، يتم توفير إطار قانوني يشجع على تبادل المعلومات والخبرات والممارسات الأفضل في مجال الأمن السيبراني، وهذا يعزز فعالية الجهود المشتركة للتصدي للتهديدات السيبرانية.

4- حماية المعلومات الحساسة:

تهدف تشريعات الهيئة الوطنية للأمن السيبراني إلى حماية المعلومات الحساسة في المملكة العربية السعودية. وتشمل هذه التشريعات تدابير لتنظيم جمع ومعالجة وتخزين ونقل المعلومات الحساسة بطرق آمنة ومحمية. وبالتالي، فإنها تساهم في حماية خصوصية الأفراد والشركات وتحمي المعلومات الحساسة مثل المعلومات الشخصية والمالية والتجارية من الوصول غير المصرح به والاستخدام غير القانوني.

5- تعزيز الثقة الرقمية:

تسهم تشريعات الهيئة الوطنية للأمن السيبراني في تعزيز الثقة الرقمية في المملكة العربية السعودية. ومن خلال تحقيق أمن وسلامة البيانات والأنظمة السيبرانية، يتم بناء بيئة رقمية موثوقة تشجع على التبادل الإلكتروني للمعلومات وتعزز الاعتماد على الخدمات الرقمية. وهذا يدعم التحول الرقمي والابتكار ونمو الاقتصاد الرقمي في المملكة.

كما ترى الباحثة أن تشريعات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية تلعب دوراً حاسماً في تحقيق الأمن السيبراني وحماية البنية التحتية السيبرانية والمعلومات الحساسة. وتوفر هذه التشريعات الإطار القانوني اللازم للأنشطة الوقائية والتحقيقية والتنظيمية لمكافحة التهديدات السيبرانية (الهيئة الوطنية للأمن السيبراني، 2018، ص 89-91).

8- طرق تعزيز الأمن السيبراني في المملكة العربية السعودية:

تحدد سبل تعزيز الأمن السيبراني في المملكة العربية السعودية، في المستويات التالية:

1- الإدارة: على الإدارات العامة والخاصة توحيد جهودها بهدف وضع استراتيجية وطنية لأمن الفضاء

السيبراني تشمل التالي:

- وضع أسس التعاون الوطني بين القطاعات العامة والخاصة

- خلق القدرات الوطنية لإدارة الحوادث من الكوارث السيبرانية، وتعزيز جوانب الصمود في إدارة استمرارية الأعمال عبر إنشاء مركز وظيفي للاستجابة من الحوادث وابداء الدعم اللازم
 - إنشاء مركز تعافي من الكوارث واستمرارية الأعمال
 - نشر ثقافة وطنية توعوية بمفاهيم الأمن السيبراني ومخاطره
 - تعزيز حماية الفضاء الالكتروني الحكومي
 - التنسيق والتعاون مع الجهات الاقليمية والدولية ذات العلاقة (القحطاني ، 2019 ، ص47-49).
- 2- المؤسسات والشركات: على المؤسسات والشركات الخاصة العمل على التالي:
- ضمان الموارد الضرورية المخصصة لتخطيط واعتماد انظمة حماية متعددة الطبقات لردع المخاطر عن أنظمة المعلومات والبنى التحتية التابعة لهم.
 - تنفيذ وتطبيق عمليات واجراءات أمنية واعتبارها مهمة إلزامية ذات أولوية عالية (القحطاني ، 2019 ، ص55-).
- 3- الجامعات والتعليم الأكاديمي: للجامعات دور اساسي في تأمين الدعم الأكاديمي المطلوب لتحفيز علم الأمن السيبراني عبر:
- إجراء بحوث أكاديمية متطورة حول الجوانب التقنية لأمن الشبكات والمعلومات.
 - خلق بروتوكولات أمنية جديدة وحلول حسابية.
 - إدراج مخاطر الأمن السيبراني وسبل مكافحتها لا سيما الجوانب القانونية لمواجهة الجرائم الالكترونية في المقررات التعليمية الجامعية (الخالدي، 2016، ص159).
- 4- المواطن السعودي: على المواطن السعودي أن يصبح أكثر وعياً وإدراكاً وان يتعلم كيف يكون أكثر يقظة فيما يتعلق بالحفاظ على امن عملياته الشخصية. كما عليه أن يصبح أكثر دراية بالخطوات الأساسية لحماية معلوماته الشخصية والمعلومات المتعلقة بعائلته والمؤسسات التي يعمل بها (الخالدي ، 2016 ، ص114).
- وهناك العديد من أنواع التدابير التي ينبغي توطيدها لزيادة أمن البنية التحتية للاتصالات وتكنولوجيا المعلومات، من بينها:
- بناء الوعي وتثقيف وتدريب جميع أصحاب المصلحة في الأمن السيبراني.
 - خلق وحدات يمكنها أن تؤدي وظيفة المركز الوطني للإنذار المبكر والاستجابة للأزمات، وتجميع الموارد الضرورية لأداء ذلك بفعالية وتقاسمها عبر العديد من البلدان لخدمة إقليم ما.
 - إنشاء المراقبة والتفتيش (الشبهة ما تكون بنقاط التفتيش على الطرق).
 - بناء الخبرة داخل فريق شرطة سيبراني يمكنه المساهمة في عملية تعاونية دولية للبحث في الجريمة المرتبطة بالحاسوب والمحاكمات الخاصة بذلك.

- بلورة حلول تكنولوجية لإدارة الهوية، والتحكم في النفاذ، واستخدام العتاد الآمن للحاسوب، والأنظمة الأساسية للبرمجيات، والبنى التحتية المساندة، وبرتوكولات التشفير والإدارة التشغيلية (الغامدي، 2021، ص 58-60).

وينبغي أن تستهدف استراتيجية أمن البنى التحتية الرقمية بتحليل المخاطر المرتبطة بمعالجة المعلومات، والاتصالات والفضاء السيبراني وذلك كجزء من عملية إدارة المخاطر. ويحتاج الأمر إلى تحديد المخاطر الأمنية لتكنولوجيا المعلومات (التي يشار إليها أيضاً كمخاطر الحاسوب، أو مخاطر المعلومات أو مخاطر التكنولوجيا) إلى جانب جميع المخاطر الأخرى التي تواجه المنظمة. فمخاطر تكنولوجيا المعلومات مخاطر تشغيلية تحتاج إلى السيطرة عليها. ومن الضروري عند البت في المستوى المرغوب فيه من الحماية وأنواع تدابير الأمن التي يجب تحقيقها الموازنة بين حجم المخاطر (من الناحية المالية) وبين التكاليف التي قد تلزم للتقليل منها وكحد أدنى، يجب تحديد الأصول التي يجب حمايتها وذلك كحد أدنى، بالإضافة إلى مسوغات حمايتها، تبعاً للعقبات الفعلية والموارد التنظيمية والمالية والبشرية والتقنية المتوفرة. وينبغي للتدابير المتخذة أن تكون فعالة كما يجب أن تعكس توازناً بين الأداء وبين الفعالية التكاليفية. فالسيطرة على مخاطر تكنولوجيا المعلومات، بالنسبة لمنظمة ما، تعني بلورة استراتيجية تعرف سياسة عامة للأمن وتبت بشأن تنفيذها من الناحيتين التكتيكية والتشغيلية (الاتحاد الدولي للاتصالات، 2019، ص 176-178).

كما يجب تحديث وتعزيز التشريعات المتعلقة بالأمن السيبراني لتكون متطابقة مع التهديدات الجديدة والتطورات التكنولوجية؛ كأن تتضمن هذه التشريعات إجراءات صارمة لمكافحة الاختراقات والهجمات السيبرانية، وتحدد المسؤوليات والواجبات للمؤسسات والجهات ذات الصلة.

الفصل الثالث

إجراءات البحث (المنهجية والإجراءات)

3-1 منهج البحث:

اعتمدت الباحثة على المنهج الوصفي التحليلي لمعرفة السبل المساعدة لإدارة مخاطر الأمن السيبراني في الشركات السعودية التقنية بحسب تشريعات الهيئة الوطنية للأمن السيبراني.. ويعرف المنهج الوصفي التحليلي بأنه منهج يساعد الباحثين في جمع المعلومات والبيانات، مع إيجاد وسائل مختلفة لتفسيرها. ويمكن عن طريق المنهج الوصفي التحليلي أن يربط الباحث بين العلاقات؛ من خلال طرح أسئلة. ويستطيع الباحث من خلال المنهج الوصفي التحليلي استخراج النتائج وفقاً لشواهد وقرائن متنوعة.

3-2 مجتمع وعينة البحث:

تمثل مجتمع الدراسة في منسوبي المؤسسات التكنولوجية في منطقة شرق الرياض والبالغ عددهم (370) موظف وموظفة (الهيئة العامة للإحصاء، 1444، ص 96). وبلغت حجم عينة الدراسة (120) مفحوص من منسوبي المؤسسات التكنولوجية في منطقة شرق الرياض. وتم اختيار العينة بالطريقة العشوائية عن طريق وضع الأسماء على جهاز الحاسب الآلي والاختيار من بينها، وقامت الباحثة بتصميم إستبانة إلكترونية لتحقيق أهداف الدراسة.

3-3 أداة البحث:

قامت الباحثة بتصميم إستبانة من خلال النظر إلى الأدبيات والدراسات السابقة، ثم قامت بتطويرها لتحقيق أهداف الدراسة الحالية، وتكونت أداة الدراسة من قسمين، نوضحها كما يلي:

القسم الأول: البيانات الشخصية، ويشمل على ثلاثة أبعاد رئيسية:

- العمر
- المؤهل الوظيفي
- المستوى الوظيفي
- الخبرة العملية
- مجال العمل أو التخصص

القسم الثاني: محاور الاستبانة، واشتملت على ثلاثة أبعاد رئيسية:

المحور الأول: أسباب مخاطر الأمن السيبراني في المملكة العربية السعودية

المحور الثاني: أهمية الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني

المحور الثالث: طرق تطوير إدارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني

واستخدمت الباحثة مقياس ليكرت الخماسي للتعرف على إستجابات عينة الدراسة لفقرات الإستبانة، والجدول التالي يوضح بدائل الإستجابات:

جدول رقم (1)

مقياس ليكرت الخماسي

المعيار	موافق بشدة	موافق	إلى حد ما	غير موافق	غير موافق بشدة
الدرجة	5	4	3	2	1
المتوسط الحسابي	5.00-4.20	4.19-3.40	3.39-2.60	2.59-1.80	1.79-1.00
درجة الموافقة	مرتفعة جداً	مرتفعة	متوسطة	منخفضة	منخفضة جداً

3-4 أداة البحث:

اعتمدت الباحثة للتحقق من صدق الأدوات على طريقتين، الأولى وتسمى الصدق الظاهري (Face validity)، والثانية وتسمى الاتساق الداخلي (Internal Consistency).

• الصدق الظاهري:

- وهو الصدق المعتمد على المحكمين، حيث تم عرض أداة الدراسة على عدد من عدد من الخبراء والمتخصصين بلغ عددهم (ثلاثة) محكمين طلب منهم دراسة الأداة وإبداء آرائهم فيها من حيث:
 - مدى ارتباط كل فقرة من فقراتها بالبعد الذي تنتهي إليه.
 - مدى وضوح كل فقرة وسلامة صياغتها اللغوية.
 - ملاءمتها لتحقيق الهدف الذي وضعت من أجله، واقتراح طرق تحسينها وذلك بالحذف أو الإضافة أو إعادة الصياغة أو غير ما ورد مما يرويه مناسباً.

وقد قدموا ملاحظات قيمة أفادت الدراسة، وأثرت الأداة، وساعدت على إخراجها بصورة جيدة. وبذلك تكون الادوات قد حققت ما يسمى بالصدق الظاهري أو المنطقي.

• صدق الاتساق الداخلي لأداة الدراسة:

تم حساب صدق الاتساق الداخلي بحساب معامل ارتباط بيرسون بين درجة كل فقرة والدرجة الكلية للبعد الذي تنتهي إليه كما توضح نتائجها الجدول التالي:

جدول رقم (3-2)

معاملات ارتباط بيرسون بين درجات كل فقرة والدرجة الكلية للبعد الذي تنتهي إليه

المحور الأول		المحور الثاني		المحور الثالث	
م	معامل الارتباط	م	معامل الارتباط	م	معامل الارتباط
1	*0.528	1	*0.718	1	*0.966
2	*0.802	2	*0.877	2	*0.932
3	*0.808	3	*0.925	3	*0.940
4	*0.769	4	*0.957	4	*0.952
5	*0.626	5	*0.835	5	*0.952
6	*0.707	6	*0.960	6	*0.916
7	*0.766	7	*0.949	7	*0.973
8	*0.949	8	*0.960	8	*0.965
9	*0.964	9	*0.966	9	*0.938
10	*0.958	10	*0.955	10	*0.986

يلاحظ من الجدول السابق أن معاملات ارتباط كل فقرة من فقرات أداة الدِّراسة (الاستبانة) والدرجة الكلية للبعد الذي تنتهي إليه جاءت جميعها داله إحصائيا عند مستوى دلالة (0.05)، مما يدل على توافر عالية من صدق الاتساق الداخلي لأداة الدِّراسة (الاستبانة). وقامت الباحثة باستخراج معاملات الارتباط بين درجة كل بعد والدرجة الكلية للاستبانة وكانت النتائج كالتالي:

جدول رقم (3-3)

معاملات الارتباط بين درجة كل بعد والدرجة الكلية للاستبانة

المحور	معامل الارتباط
المحور الأول : اسباب مخاطر الأمن السيبراني في المملكة العربية السعودية	*0.978
المحور الثاني : أهمية الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني	*0.888
المحور الثالث : طرق تطوير ادارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني	*0.900

* وجود دلالة عند مستوى (0.05)

يتضح من الجدول السابق أن قيم معاملات الارتباط جاءت بقيم مرتفعة حيث تراوحت بين (0.888 – 0.978)، وكانت جميعها داله إحصائيا عند مستوى دلالة (0.05) مما يعني وجود درجة عالية من الصدق البنائي للاستبانة.

3-5 اثبات أداة البحث:

للتحقق من ثبات الاستبانة استخدمت الباحثة معادلة ألفا كرونباخ ويوضح الجدول التالي معاملات الثبات الناتجة باستخدام هذه المعادلة:

جدول رقم (3-4)

معاملات ثبات أداة الدراسة

المعامل	عدد	البعد
الفكرونباخ	العبارات	
0.829	10	المحور الأول: اسباب مخاطر الأمن السيبراني في المملكة العربية السعودية
0.966	10	المحور الثاني: أهمية الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني
0.982	10	المحور الثالث: طرق تطوير ادارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني
0.984	30	الاستبانة ككل

يتضح من الجدول السابق أن قيم معاملات الثبات للأبعاد جاءت بقيم عالية حيث تراوحت بين (0.829-0.982) وبلغ معامل الثبات الكلي للاستبانة (0.984).

3-6 الأساليب الإحصائية

1- استخدمت الباحثة برنامج التحليل الإحصائي (Statistical Package for the Social Sciences) (SPSS)، حيث استخدمت الباحثة الأساليب الإحصائية التالية لاستخراج النتائج:

1. التحليل الوصفي: ويشمل:

- النسب المئوية (Percentages) والتكرارات (Frequencies) والمتوسطات الحسابية لوصف عينة الدراسة.

- معامل ألفا كرونباخ (Cronbach Alpha) للتأكد من ثبات فقرات الإستبانة.

- معامل ارتباط بيرسون (Pearson Correlation Coefficient) لتأكد من صدق الاتساق الداخلي للمقياس من خلال استخراج معامل بيرسون بين كل بعد والدرجة الكلية للمقياس.

بالإضافة إلى ما سبق استخدامه لتقنين أداة الدراسة مثل معامل الارتباط لـ "بيرسون" (Person Product-moment correlation)، ومعامل "ألفا كرونباخ" (Cronbach Alpha)، فإنه تم استخدام الأساليب الإحصائية التالية:

الإحصاء الوصفي: وذلك من خلال:

- التكرارات والنسب المئوية لوصف مجتمع الدراسة بالنسبة للمعلومات الأولية.

- المتوسط الحسابي وذلك لحساب المتوسط الحسابي لكل فقرة ولكل بعد.
- الانحرافات المعيارية للتعرف على التباين لل فقرات وللأبعاد.
- معادلة المدى لمقياس ليكارت الخماسي لتحديد الدرجة ، كما في الجدول التالي:

جدول (3-5)

الوزن النسبي للدرجات

الوزن	الدرجة
1	منخفضة جداً
2	منخفضة
3	متوسطة
4	عالية
5	عالية جداً

ثم يتم تحديد الاتجاه لمقياس ليكارت الخماسي كما في الجدول التالي:

جدول (3-6) المتوسط المرجح للدرجات

الوزن	الدرجة
1	منخفضة جداً
2	منخفضة
3	متوسطة
4	عالية
5	عالية جداً

الفصل الرابع

نتائج الدراسة الميدانية:

4-1 مقدمة:

هدف البحث إلى التعرف على سبل مساعدة لإدارة مخاطر الأمن السيبراني في الشركات السعودية التقنية بحسب تشريعات الهيئة الوطنية للأمن السيبراني، ولبحث تساؤلات البحث تم بناء استبانة شملت هذه المتغيرات، وتم تطبيقها على أفراد عينة الدراسة البالغ عددهم (120) مفحوص من منسوبي المؤسسات التكنولوجية في منطقة شرق الرياض، وتم اختيار العينة بالطريقة العشوائية، وقامت الباحثة بتصميم استبانة إلكترونية لتحقيق أهداف الدراسة. وقد تم إدخال البيانات إلى جهاز الحاسب الآلي وباستخدام البرنامج الإحصائي SPSS تم تحليل النتائج.

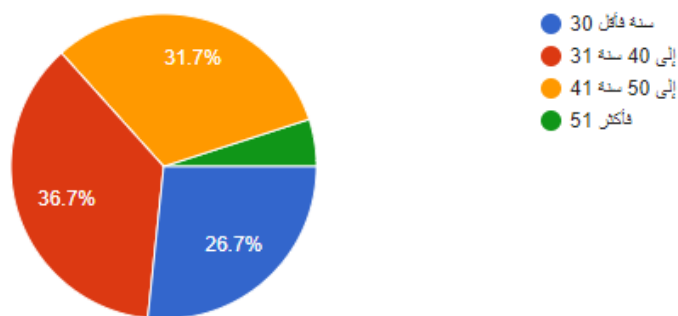
4-2 خصائص عينة الدراسة:

1- حسب العمر

جدول (4-1) توزيع عينة الدراسة حسب العمر

العمر	التكرار	النسبة
30 سنة فأقل	32	26.7%
40-31	44	36.7%
50-41	38	31.7%
51 فأكثر	6	5%
المجموع	120	100%

يتضح من الجدول السابق أن أعلى نسبة في توزيع عينة الدراسة حسب العمر، هي: 40-31 بنسبة 36.7%، ثم 30-40 بنسبة 36.7%، ثم 30 سنة فأقل بنسبة 26.7%، ثم 51 فأكثر بنسبة 5%. كما يوضح الشكل التالي:



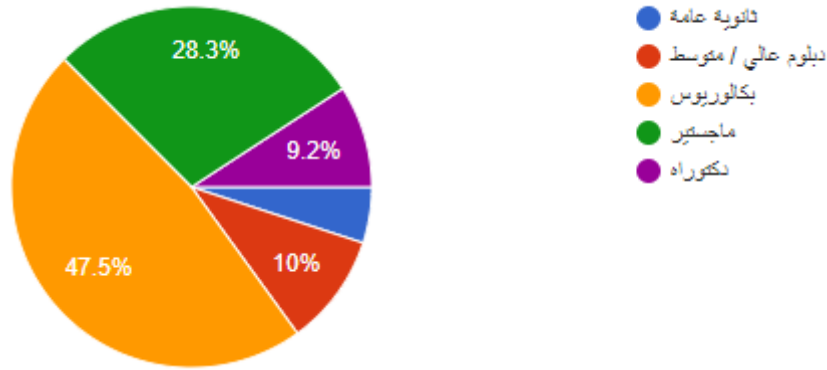
الشكل رقم (1) توزيع عينة الدراسة حسب العمر

2- حسب المؤهل العلمي

جدول (4-2) توزيع عينة الدراسة حسب المؤهل العلمي

المؤهل العلمي	التكرار	النسبة
ثانوية عامة	6	5%
دبلوم عالي / متوسط	12	10%
بكالوريوس	57	47.5%
ماجستير	34	28.3%
دكتوراه	11	9.2%
المجموع	120	100%

يتضح من الجدول السابق أن أعلى نسبة في توزيع عينة الدراسة حسب الخبرة هي : بكالوريوس بنسبة 47.5%، ثم ماجستير بنسبة 28.5%، ثم دبلوم عالي / متوسط بنسبة 10%، ثم دكتوراه بنسبة 9.2%، ثم ثانوية عامة بنسبة 5%. ويتضح ذلك من الشكل التالي:



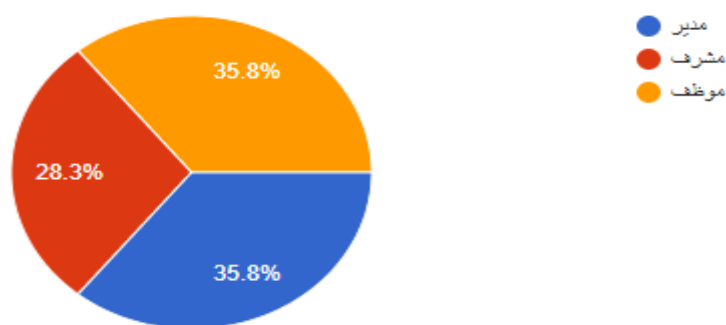
الشكل رقم (2) توزيع عينة الدراسة حسب المؤهل العلمي

3- حسب المستوى الوظيفي

جدول (4-3) توزيع عينة الدراسة حسب المستوى الوظيفي

النسبة	التكرار	المستوى الوظيفي
35.8%	43	مدير
28.3%	34	مشرف
35.8%	43	موظف
100%	120	المجموع

يتضح من الجدول السابق أن أعلى نسبة في توزيع عينة الدراسة حسب المستوى الوظيفي هي: مدير وموظف بنسبة 35.8% لكل منهما ثم مشرف بنسبة 28.3%. ويتضح ذلك من الشكل التالي:



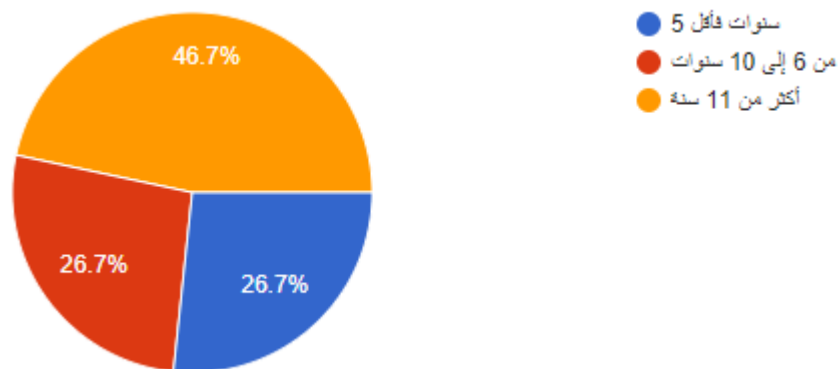
الشكل رقم (3) توزيع عينة الدراسة حسب المستوى الوظيفي

4- حسب الخبرة العملية

جدول (4-4) توزيع عينة الدراسة حسب الخبرة العملية

النسبة	التكرار	الخبرة العملية
26.7%	32	5 سنوات فأقل
26.7%	32	6-10
46.7%	56	أكثر من 11 سنة
100%	120	المجموع

يتضح من الجدول السابق أن أعلى نسبة في توزيع عينة الدراسة حسب الخبرة العملية هي: أكثر من 11 سنة بنسبة 46.7%، ثم 5 سنوات فأقل ، و 6-10 بنسبة 26.7% لكل منهما. ويتضح ذلك من الشكل التالي:



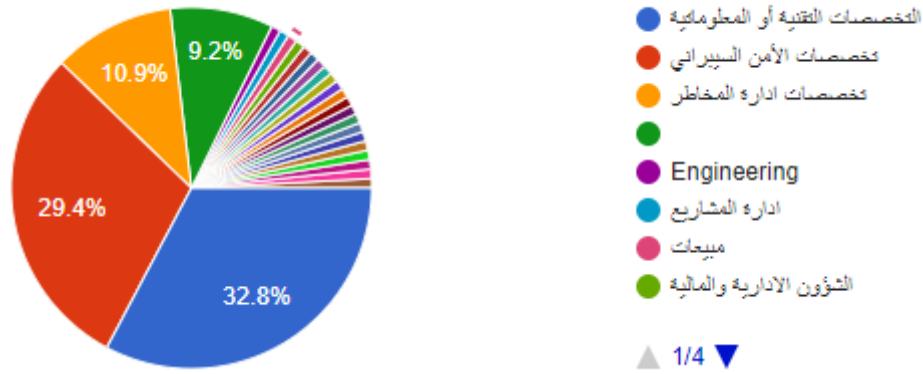
الشكل رقم (4) توزيع عينة الدراسة حسب الخبرة العملية

5- حسب مجال العمل / التخصص

جدول (4-5) توزيع عينة الدراسة حسب مجال العمل/ التخصص

النسبة	التكرار	مجال العمل/ التخصص
29.4%	35	تخصصات الأمن السيبراني
32.8%	39	التخصصات التقنية
10.9%	13	ادارة المخاطر
9.2%	11	تخصص هندسي
5%	6	إدارة الأبحاث
12.7%	16	الشؤون الادارية والمالية
100%	120	المجموع

يتضح من الجدول السابق أن أعلى نسبة في توزيع عينة الدراسة حسب مجال العمل هي: التخصصات التقنية بنسبة 32.8%، ثم تخصصات الأمن السيبراني بنسبة 29.4%، ثم الشؤون الإدارية والمالية بنسبة 12.7%، ثم إدارة المخاطر بنسبة 10.9%، ثم تخصص هندسي بنسبة 9.2%، ثم إدارة الأبحاث بنسبة 5%. ويتضح ذلك من الشكل التالي:



الشكل رقم (5) توزيع عينة الدراسة حسب مجال العمل

وللإجابة على أسئلة الدراسة تم حساب المتوسطات الحسابية والانحرافات المعيارية للتعرف على سبل مساعدة لإدارة مخاطر الأمن السيبراني في الشركات السعودية التقنية بحسب تشريعات الهيئة الوطنية للأمن السيبراني، وكانت النتائج كالتالي:

جدول (4-6) المتوسطات الحسابية والانحرافات المعيارية لأبعاد سبل مساعدة لإدارة مخاطر الأمن السيبراني في الشركات السعودية التقنية بحسب تشريعات الهيئة الوطنية للأمن السيبراني

رقم البعد	البعد	المتوسط الحسابي	النسبة المئوية	الانحراف المعياري	ترتيب البعد	الدرجة
1	المحور الأول: اسباب مخاطر الأمن السيبراني في المملكة العربية السعودية	3.55	64%	0.893	3	مرتفعة
2	المحور الثاني: أهمية الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني	3.73	68%	0.771	1	مرتفعة

3	المحور الثالث : طرق تطوير ادارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني	3.71	٪68	0.819	2	مرتفعة
	سبل مساعدة لإدارة مخاطر الأمن السيبراني في الشركات السعودية التقنية بحسب تشريعات الهيئة الوطنية للأمن السيبراني	3.66	٪66	0.793		مرتفعة

يتبين من الجدول السابق أن محاور سبل مساعدة لإدارة مخاطر الأمن السيبراني في الشركات السعودية التقنية بحسب تشريعات الهيئة الوطنية للأمن السيبراني ، جاءت بدرجة (مرتفعة)، حيث جاء المتوسط العام للمجموع الكلي (3.66)، بانحراف معياري (0.793). نظرا لوجهة نظر عينة الدراسة لأهمية إدارة مخاطر الأمن السيبراني في الشركات السعودية التقنية بحسب تشريعات الهيئة الوطنية للأمن السيبراني.

3-4: نتائج الدراسة الميدانية

وتم تطبيق الاستبيان التالي بعد تحكيمة ، وتكون من ثلاث محاور ، وهي: المحور الأول : اسباب مخاطر الأمن السيبراني في المملكة العربية السعودية، المحور الثاني : أهمية الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني ، المحور الثالث : طرق تطوير ادارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني. (أنظر ملحق.....).

محاور الدراسة:

المحور الأول : اسباب مخاطر الأمن السيبراني في المملكة العربية السعودية
قامت الباحثة بتخصيص (10) عبارات لتحديد اسباب مخاطر الأمن السيبراني في المملكة العربية السعودية ، وكانت النتائج كالتالي:

جدول (4-7) المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات اسباب مخاطر الأمن السيبراني في المملكة العربية السعودية مرتبة تنازليا حسب المتوسطات الحسابية

م	العبارة	المتوسط الحسابي	النسبة المئوية	الانحراف المعياري	الدرجة	الترتيب
3	التصيد الإلكتروني عبر الإنترنت مثل الرسائل الاحتيالية، وسرقة الحسابات البنكية	3.79	٪70	0.976	مرتفعة	1

7	انتهاكات الخصوصية وتسريب المعلومات الشخصية للأفراد	3.69	٪67	1.047	مرتفعة	2
4	الهجمات التي تستهدف إعاقة البنية التحتية السيبرانية للمملكة، مثل تعطيل خدمات الإنترنت	3.64	٪66	0.932	مرتفعة	3
8	الهجمات السيبرانية على البنية التحتية الحيوية مثل الشبكات الكهربائية والماء والنقل	3.62	٪65	1.058	مرتفعة	4
1	هجمات القرصنة الإلكترونية ومحاولات اختراق الأنظمة السيبرانية والحصول على معلومات حساسة أو التلاعب بها	3.57	٪64	1.039	مرتفعة	5
6	تهديدات البرمجيات الخبيثة والفايروسات التي يتم استخدامها لاختراق الأنظمة وتدمير البيانات أو سرقتها	3.50	٪63	1.042	مرتفعة	6
9	الاختيال المصرفي وسرقة المعلومات المالية مما يتسبب في خسائر مالية كبيرة	3.48	٪62	1.042	مرتفعة	7
2	سرقة المعلومات الحساسة والتجسس على الأنشطة الحكومية والخاصة	3.48	٪62	1.087	مرتفعة	8
5	الاختراقات السيبرانية أو الأمنية للمؤسسات الحكومية والشركات والتي تهدد سرية المعلومات والملكية الفكرية وسلامة الأنظمة	3.43	٪61	0.991	مرتفعة	9
10	تهديدات الهجمات السيبرانية على البنية الحيوية الوطنية مثل القطاعات النفطية والنقل والصناعة	3.41	٪60	0.983	مرتفعة	10
اسباب مخاطر الأمن السيبراني في المملكة العربية السعودية		3.55	٪64	0.893	مرتفعة	

من خلال الجدول الموضح أعلاه يتضح ان عبارات اسباب مخاطر الأمن السيبراني في المملكة العربية السعودية ، جاءت بدرجة (مرتفعة) حيث بلغ المتوسط الحسابي الكلي (3.55 من 5) وهو متوسط يقع ضمن الفئة الرابعة من فئات مقياس ليكرت الخماسي (3.40 إلى 4.19) وهي الفئة التي تشير إلى درجة (مرتفعة). كما يتضح من النتائج أن هناك تفاوتاً في استجابات أفراد عينة الدراسة على عبارات اسباب مخاطر الأمن السيبراني في المملكة العربية السعودية ، حيث تراوحت المتوسطات ما بين (3.41 إلى 3.79 من 5) وهي متوسطات تقع ضمن الفئتين الثالثة والرابعة من فئات مقياس ليكرت الخماسي وتشير إلى درجة (متوسطة، مرتفعة) على التوالي. كما يوضح الجدول السابق، ما يلي:

- جاءت العبارة (التصيد الإلكتروني عبر الإنترنت مثل الرسائل الاحتيالية، وسرقة الحسابات البنكية) بالمرتبة الأولى بدرجة (مرتفعة) بمتوسط حسابي (3.79) ونسبة مئوية بلغت (70٪).
 - جاءت العبارة (تهديدات الهجمات السيبرانية على البنية الحيوية الوطنية مثل القطاعات النفطية والنقل والصناعة) بالمرتبة العاشرة بدرجة (مرتفعة)، بمتوسط حسابي (3.41) ونسبة مئوية بلغت (60٪).
- وتفسر الباحثة حصول العبارة (التصيد الإلكتروني عبر الإنترنت مثل الرسائل الاحتيالية، وسرقة الحسابات البنكية) على الترتيب الأول بدرجة (مرتفعة) إلى مدى إدراك عينة الدراسة لخطورة التصيد الإلكتروني عبر الإنترنت مثل الرسائل الاحتيالية، وسرقة الحسابات البنكية وتتفق تلك النتائج مع دراسة الصيدلاني (2017) التي أوضحت نتائجها أنه في حين تقع مسؤولية توعية الطلبة بحقوق الملكية الفكرية ومخاطر القرصنة على قطاع التعليم فإن توعية عامة الشعب بمختلف مستوياتهم تقع على عاتق الحكومة والقطاع الخاص. والتأكيد بأن زيادة الوعي مفتاح القدرة على الحد من ظاهرة القرصنة. كما تتفق تلك النتائج مع دراسة ستيفن Stephen (2017) التي أوضحت نتائجها تقديم اقتراح ببعض الحلول للحد من الظاهرة في المدارس مثل توعية الطلبة والمدرسين بالمسؤوليات والقيود الواجب مراعاتها عند استخدام البرمجيات، إضافة إلى جعل السياسات المتعلقة بقرصنة البرمجيات جزءاً من سياسات حقوق الطبع لفائدتها على الرغم من كلفتها العالية. كما تتفق تلك النتائج مع دراسة والدو Waldo (2018) التي أوضحت نتائجها أن استراتيجية الرحلات المعرفية عبر الويب القائمة على محاكاة خصوصية البيانات تسهل على الجهات الأمنية التوعية بخصوصية المعلومات ومصادر المعرفة المتاحة، على شبكة الإنترنت.

المحور الثاني : أهمية الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني

قامت الباحثة بتخصيص (10) عبارات لتحديد أهمية الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني ، وكانت النتائج كالتالي:

جدول (4-8) المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات أهمية الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني مرتبة تنازلياً حسب المتوسطات الحسابية

م	العبرة	المتوسط الحسابي	النسبة المئوية	الانحراف المعياري	الدرجة	الترتيب
8	الاستثمار لتطوير تقنيات تعزيز الأمن السيبراني	4.12	٪78	0.861	مرتفعة	1
9	التعاون بشكل وثيق مع الهيئة الوطنية للأمن السيبراني في تنفيذ الضوابط والتشريعات الأمنية اللازمة	3.95	٪74	0.909	مرتفعة	2
4	تحديد واعتماد وثيقة لسياسات واجراءات الأمن السيبراني ويتم تطبيقها بشكل منتظم	3.86	٪71	0.843	مرتفعة	3
5	العمل على اعداد وتقديم تقارير مفصلة عن الاستجابة للحوادث السيبرانية وتحليلها ومشاركتها مع أصحاب العلاقة	3.71	٪68	1.066	مرتفعة	4
6	العمل على المراجعات الدورية لتحقيق من الامتثال لتشريعات الهيئة الوطنية للأمن السيبراني	3.69	٪67	0.975	مرتفعة	5
3	انشاء برنامج خاص بالتوعية بالأمن السيبراني، بالإضافة إلى الاستثمار في تدريب الموظفين حول قضايا الأمن السيبراني	3.64	٪66	0.983	مرتفعة	6
1	تعيين فريق متخصص في الأمن السيبراني	3.62	٪65	0.854	مرتفعة	7
7	التعاون مع القطاعات الخاصة والحكومية في المملكة لتبادل المعلومات والمنفعة لتعزيز الأمن السيبراني	3.60	٪65	1.127	مرتفعة	8
10	توثيق واعتماد استراتيجية للأمن السيبراني تتضمن الأهداف والمبادرات والمشاريع الخاصة في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة	3.36	٪59	0.906	متوسطة	9
2	اعداد تقارير دورية عن تقييمات الأمن السيبراني وتحديد نقاط الضعف وخطط المعالجة	3.32	٪57	0.901	متوسطة	10

أهمية الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني	3.73	68%	0.771	مرتفعة
--	------	-----	-------	--------

من خلال الجدول الموضح أعلاه يتضح ان عبارات محور أهمية الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني ، جاءت بدرجة (مرتفعة) حيث بلغ المتوسط الحسابي الكلي (3.73 من 5) وهو متوسط يقع ضمن الفئة الرابعة من فئات مقياس ليكرت الخماسي (3.40 إلى 4.19) وهي الفئة التي تشير إلى درجة (مرتفعة). كما يتضح من النتائج أن هناك تفاوتاً في استجابات أفراد عينة الدراسة على عبارات محور أهمية الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني ، حيث تراوحت المتوسطات ما بين (3.32 إلى 4.12 من 5) وهي متوسطات تقع ضمن الفئتين الثالثة والرابعة من فئات مقياس ليكرت الخماسي وتشير إلى درجة (متوسطة، مرتفعة) على التوالي. كما يوضح الجدول السابق ما يلي:

- جاءت العبارة (الاستثمار لتطوير تقنيات تعزيز الأمن السيبراني) بالمرتبة الأولى بدرجة (مرتفعة) بمتوسط حسابي (4.12) ونسبة مئوية بلغت (78%).
 - جاءت العبارة (اعداد تقارير دورية عن تقييمات الأمن السيبراني وتحديد نقاط الضعف وخطط المعالجة) بالمرتبة العاشرة بدرجة (متوسطة) بمتوسط حسابي (3.32) ونسبة مئوية بلغت (57%).
- وتفسر الباحثة حصول العبارة (الاستثمار لتطوير تقنيات تعزيز الأمن السيبراني) على الترتيب الأول بدرجة (مرتفعة) إلى خبرة عينة الدراسة وما لمسوه خلال واقع عملهم.
- وتتفق تلك النتائج مع دراسة الزهراني (2018) التي أوضحت نتائجها أن من أسباب انخفاض نسبة القرصنة في بعض الدول وجود حماية قوية للاختراعات والبرامج وحقوق الملكية الفكرية ، عكس الحال في كثير من الدول النامية. كما تتفق تلك النتائج مع دراسة العضياني (2018) التي أوضحت نتائجها أن اختراق أنظمة المعلومات و نظم الشبكات و المواقع المعلوماتية أصبح خطراً يقلق العديد من المنظمات ، إن هناك ارتفاعاً واضحاً في معدل الإختراقات مع تنوع الوسائل المستخدمة في الاختراق على الرغم من سبل الحماية التي تتبعها المنظمات. كما تتفق تلك النتائج مع دراسة فايز (2019) التي أوضحت نتائجها أن تكنولوجيا المعلومات تعمل على تطوير أداء الموارد البشرية بالشركة ، و أبدى أغلبية عينة الدراسة (98% منهم) شعورهم الإيجابي بأهمية التدريب .
- المحور الثالث : طرق تطوير ادارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني**
- قامت الباحثة بتخصيص (10) عبارات لتحديد طرق تطوير ادارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني. وكانت النتائج كالتالي:

جدول (4-9) المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات طرق تطوير ادارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني مرتبة تنازلياً حسب المتوسطات الحسابية

م	العبارة	المتوسط الحسابي	النسبة المئوية	الانحراف المعياري	الدرجة	الترتيب
4	تعيين فريق مختص للتعامل مع حوادث الأمن السيبراني والاستجابة السريعة لها	3.86	٪71	0.872	مرتفعة	1
1	تعزيز الوعي بأهمية الأمن السيبراني وتدريب الموظفين على المخاطر والتهديدات السيبرانية	3.79	٪70	1.001	مرتفعة	2
2	حوكمة الأمن السيبراني من خلال تطوير وإنشاء سياسات واجراءات خاصة بالأمن السيبراني، بالإضافة إلى تحديد اطار عمل لادارة مخاطر الأمن السيبراني وضمان تطبيقهم بشكل فعال	3.79	٪70	0.871	مرتفعة	3
6	انشاء لجنة اشرافية متخصصة للأمن السيبراني لعرض ومناقشة الوضع السيبراني، وضمان مراجعة تطبيق المتطلبات التشريعية بشكل دوري وابداء الدعم اللازم	3.74	٪68	0.912	مرتفعة	4
7	تبني البحث والتطوير في مجال الأمن السيبراني ودعم الجهود التعليمية لتأهيل المتخصصين في هذا المجال	3.71	٪68	0.918	مرتفعة	5
5	تعزيز التعاون والتنسيق بين القطاعات العامة والخاصة والهيئات الأخرى في المملكة، بالإضافة إلى توسيع التعاون مع المنظمات الدولية الأمنية	3.69	٪67	0.869	مرتفعة	6
3	تعيين ذوي الخبرة لأعمال تحديد وتقييم المخاطر السيبرانية وتحليل الثغرات الأمنية في الأنظمة والشبكات والاشراف على تحقيق الامتثالات التشريعية للمشاريع التقنية	3.67	٪67	0.928	مرتفعة	7

10	التواصل والاشتراك مع مصادر موثوقة فيما يتعلق بالتنبيهات الخاصة بالثغرات الجديدة والمحدثة، وتبليغ الهيئة الوطنية للأمن السيبراني عند حدوث حادثة أمن سيبراني	3.65	66%	0.926	مرتفعة	8
9	ضمان معالجة واغلاق الثغرات الأمنية بناء على تصنيفها والمخاطر السيبرانية المترتبة عليها	3.62	65%	1.035	مرتفعة	9
8	مراجعة وتحديث التشريعات القائمة لتعزيز القدرة على مكافحة الجرائم السيبرانية ومخاطر الأمن السيبراني	3.52	63%	0.994	مرتفعة	10
	طرق تطوير ادارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني	3.71	68%	0.819	مرتفعة	

من خلال الجدول السابق الموضح أعلاه يتضح ان عبارات محور طرق تطوير ادارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني، جاءت بدرجة (مرتفعة) حيث بلغ المتوسط الحسابي الكلي (3.71 من 5) وهو متوسط يقع ضمن الفئة الرابعة من فئات مقياس ليكرت الخماسي (3.40 إلى 4.19) وهي الفئة التي تشير إلى درجة (مرتفعة).

كما يتضح من النتائج أن هناك تفاوتاً في استجابات أفراد عينة الدراسة على عبارات محور طرق تطوير ادارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني ، حيث تراوحت المتوسطات ما بين (3.52 إلى 3.86 من 5) وهي متوسطات تقع ضمن الفئة الرابعة من فئات مقياس ليكرت الخماسي وتشير إلى درجة (مرتفعة). كما يوضح الجدول السابق ما يلي:

- جاءت العبارة (تعيين فريق مختص للتعامل مع حوادث الأمن السيبراني والاستجابة السريعة لها) بالمرتبة الأولى بدرجة (مرتفعة) بمتوسط حسابي (3.86) وبنسبة مئوية بلغت (71%).
 - جاءت العبارة (مراجعة وتحديث التشريعات القائمة لتعزيز القدرة على مكافحة الجرائم السيبرانية ومخاطر الأمن السيبراني) بالمرتبة العاشرة بدرجة (مرتفعة) بمتوسط حسابي (3.52) وبنسبة مئوية بلغت (63%).
- وتفسر الباحثة حصول العبارة (تعيين فريق مختص للتعامل مع حوادث الأمن السيبراني والاستجابة السريعة لها) على الترتيب الأول بدرجة (مرتفعة) إلى إدراك عينة الدراسة أهمية تعيين فريق مختص للتعامل مع حوادث الأمن السيبراني .

كما تتفق تلك النتائج مع دراسة إبداع (2019) التي أوضحت نتائجها وجود علاقة ارتباط وتأثير بين أمن المعلومات وسريتها والأداء التنافسي لشركات التأمين قيد البحث. وجاءت النتائج متطابقة مع فرضية الدراسة. كما تتفق تلك النتائج مع دراسة ليبس Lipps (2020) التي أوضحت نتائجها أن التقنيات الحديثة في تنمية الموارد البشرية تعتبر عصب الحياة العملية فهي ترفع من معنويات الفرد و تزيد فاعليته و ثقته، وتقلل من ضعفه النفسي أمام الآخرين، إن استخدام المنظمات لنظم المعلومات ذات الكفاءة والفعالية من شأنه أن يحقق لها أهدافها. كما تتفق تلك النتائج مع دراسة حمدان (2021) التي أوضحت نتائجها وجود أثر ذي دلالة إحصائية لأمن المعلومات وسريتها (الحماية المادية، حماية الأفراد، الحماية البرمجية) في الأداء المصرفي في البنوك العاملة في الأردن. كما تتفق تلك النتائج مع دراسة لerner (2021) التي أوضحت نتائجها أن التخطيط المسبق لإعداد الموارد البشرية يساعد على تلافي السلبيات ، يمكن الاعتماد على تكنولوجيا المعلومات في إعداد الموارد البشرية نظرا لفاعليتها الكبيرة.

الفصل الخامس

خلاصة لأهم نتائج الدراسة وتوصياتها:

5-1 خلاصة الدراسة:

تناولت الدراسة (5) فصول اشتمل الفصل الأول على مقدمة البحث، وفيه تناولت الباحثة، ما يلي: مقدمة البحث، المفاهيم الرئيسية في البحث، مشكلة البحث، نموذج ومتغيرات البحث، فروض البحث، أهداف البحث، أهمية البحث، حدود البحث، وهيكल البحث. وتحددت أسئلة الدراسة، فيما يلي :

1. ماهي مخاطر الأمن السيبراني في المملكة العربية السعودية؟
 2. ما مدى الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية؟
 3. ماهي سبل تطوير دور إدارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني ؟
- بينما تحددت أهداف الدراسة، فيما يلي :

1. التعرف على مخاطر الأمن السيبراني في المملكة العربية السعودية
 2. التعرف على مدى الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية.
 3. التعرف على سبل تطوير دور إدارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني.
- واشتمل الفصل الثاني على أدبيات الدراسة، أما الفصل الثالث فقد اشتمل على منهجية الدراسة إجراءاتها، وفيه تناولت الباحثة، ما يلي: منهج الدراسة، مجتمع وعينة الدراسة، أداة الدراسة وشملت صدق أداة الدراسة، وثبات أداة الدراسة، ثم أساسيات المعالجة الإحصائية. واشتمل الفصل الرابع على عرض نتائج الدراسة ومناقشتها، وفيه تناولت الباحثة تساؤلات الدراسة، وتناولت الباحثة في الفصل الخامس: خلاصة لأهم نتائج الدراسة وتوصياتها، واشتمل الفصل على ما يلي : خلاصة الدراسة، نتائج الدراسة، توصيات الدراسة، ومقترحات الدراسة.

5-2: نتائج الدراسة

- إن عبارات اسباب مخاطر الأمن السيبراني في المملكة العربية السعودية ، جاءت بدرجة (مرتفعة) حيث بلغ المتوسط الحسابي الكلي (3.55 من 5) وهو متوسط يقع ضمن الفئة الرابعة من فئات مقياس ليكرت الخماسي (3.40 إلى 4.19) وهي الفئة التي تشير إلى درجة (مرتفعة).
- إن هناك تفاوتاً في استجابات أفراد عينة الدراسة على عبارات اسباب مخاطر الأمن السيبراني في المملكة العربية السعودية ، حيث تراوحت المتوسطات ما بين (3.41 إلى 3.79 من 5) وهي متوسطات تقع ضمن الفئتين الثالثة والرابعة من فئات مقياس ليكرت الخماسي وتشير إلى درجة (متوسطة، مرتفعة) على التوالي.
- إن عبارات محور أهمية الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني ، جاءت بدرجة (مرتفعة) حيث بلغ المتوسط الحسابي الكلي (3.73 من 5) وهو متوسط يقع ضمن الفئة الرابعة من فئات مقياس ليكرت الخماسي (3.40 إلى 4.19) وهي الفئة التي تشير إلى درجة (مرتفعة).

- إن هناك تفاوتاً في استجابات أفراد عينة الدراسة على عبارات محور أهمية الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني ، حيث تراوحت المتوسطات ما بين (3.32 إلى 4.12 من 5) وهي متوسطات تقع ضمن الفئتين الثالثة والرابعة من فئات مقياس ليكرت الخماسي وتشير إلى درجة (متوسطة، مرتفعة) على التوالي.
- إن عبارات محور طرق تطوير إدارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني ، جاءت بدرجة (مرتفعة) حيث بلغ المتوسط الحسابي الكلي (3.71 من 5) وهو متوسط يقع ضمن الفئة الرابعة من فئات مقياس ليكرت الخماسي (3.40 إلى 4.19) وهي الفئة التي تشير إلى درجة (مرتفعة).
- إن هناك تفاوتاً في استجابات أفراد عينة الدراسة على عبارات محور طرق تطوير إدارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني ، حيث تراوحت المتوسطات ما بين (3.52 إلى 3.86 من 5) وهي متوسطات تقع ضمن الفئة الرابعة من فئات مقياس ليكرت الخماسي وتشير إلى درجة (مرتفعة).

3-5: توصيات الدراسة

توصي الباحثة بضرورة الاهتمام بالتوصيات التالية:

- تحديد المسؤولية المشتركة بين الإدارة التنفيذية وفريق الأمن السيبراني وجميع أعضاء المؤسسة فيما يتعلق بإدارة مخاطر الأمن السيبراني. كما يجب أن يعين مختصين ذو كفاءة عالية بالمجال وتوفير الدعم اللازم لهم لتنفيذ استراتيجيات الأمن السيبراني.
- تطوير وإنشاء سياسات وإجراءات واضحة للأمن السيبراني تتماشى مع تشريعات الهيئة الوطنية للأمن السيبراني في السعودية. كما ينبغي أن تشمل هذه السياسات والإجراءات على مجموعة من الطرق والممارسات الأمنية لحماية الأصول الرقمية ومعلومات العملاء والبيانات الحساسة الأخرى.
- تنفيذ التدابير الأمنية اللازمة لتعزيز حماية الأنظمة والشبكات والبيانات الحيوية، ويجب أن تشمل هذه التدابير مجموعة من السيطرة الفنية عن طريق تطبيق التقنيات الأمنية الفعالة مثل جدران الحماية، وأنظمة الكشف عن التسلل، وتشفير البيانات، وإدارة الهوية والوصول.
- تطوير وتطبيق برامج التوعية بالأمن السيبراني وتوفير التدريب المستمر للموظفين بشأن مخاطر الأمن السيبراني لتطبيق أفضل الممارسات للوقاية منها.
- تعزيز الوعي بأهمية حماية المعلومات الحساسة وسياسة الاستخدام المقبول وتحذير الموظفين من التهديدات السيبرانية المحتملة مثل الهجمات الاجتماعية وطرق الاحتيال الإلكترونية.
- عمل إجراء تقييم دوري لنضج الأمن السيبراني وتحليل الثغرات وتقييم العمليات الأمنية المتبعة، كما ينبغي مراجعة وتحديث السياسات والإجراءات وتحسينها بما يتوافق مع التوصيات التشريعية.
- وضع استراتيجية شاملة للأمن السيبراني تتضمن تحليل الفجوات والمخاطر السيبرانية، وتحديد الأهداف والجراءات المناسبة لكلاهما. كما يجب أن تكون هذه الاستراتيجية متوافقة مع تطلعات الشركة ومتطلبات الأعمال بما يتماشى مع التشريعات الوطنية.

- تخصيص الموارد المالية والبشرية اللازمة لتنفيذ استراتيجية الأمن السيبراني، من خلال تعيين فريق متخصص في ادارة الأمن السيبراني وتوفير التدريب المناسب لهم وتهيئة الادوات اللازمة للتعامل مع المتطلبات الأمنية لتعزيز الحماية من التهديدات السيبرانية المتطورة.
- العمل على التقييم الدوري للمخاطر السيبرانية لتحديد الثغرات ومعرفة نقاط الضعف في الأنظمة والشبكات وتحليل الآثار المحتملة للتهديدات، وتحديد أولويات الحماية لتوجيه الجهود والكوادر بشكل فعال.
- تنفيذ مجموعة من التدابير الأمنية لحماية الأنظمة والشبكات والبيانات الحساسة، ويشمل الالتزام بالتحديثات الأمنية وتطبيق السياسات والإجراءات المناسبة بحسب التوصيات المشرعة من قبل الهيئة الوطنية للأمن السيبراني.
- مراجعة وتقييم سياسات الأمن السيبراني وإجراءاتها بشكل دوري، والقيام بعمل تحليل الحوادث السيبرانية السابقة واستخلاص الدروس المستفادة لتحسين أنظمة الأمان وتعزيز القدرة على التعامل مع التهديدات المستقبلية.

4-5: مقترحات الدراسة

في ضوء النتائج التي تم التوصل اليها تقدم الباحثة بعض التوصيات لدراسات مستقبلية وذلك على النحو التالي:

- 1- تقييم فاعلية تشريعات الهيئة الوطنية للأمن السيبراني في تحقيق الأمن السيبراني في الشركات السعودية التقنية.
- 2- تحليل التهديدات السيبرانية الناشئة وتأثيرها على استراتيجيات إدارة المخاطر في الشركات السعودية التقنية.
- 3- تقنيات التحقق الثنائي كأداة لتعزيز الأمن السيبراني في الشركات السعودية التقنية: دراسة مقارنة للممارسات العالمية.
- 4- تأهيل الكوادر البشرية لإدارة مخاطر الأمن السيبراني في الشركات السعودية التقنية: تحليل الاحتياجات وتوجهات المستقبل.
- 5- تقييم تأثير الهجمات السيبراني على أداء الشركات السعودية التقنية واستراتيجيات الاستجابة المتبعة وفقاً لتشريعات الهيئة الوطنية للأمن السيبراني.

قائمة المراجع

المراجع العربية:

- الاتحاد الدولي للاتصالات. (2019). الأمن السيبراني في المملكة العربية السعودية . بيروت: مطابع الاتحاد الدولي للاتصالات.
- إبداح، باسم محمد. (2019). أمن وسرية المعلومات وأثرها على الأداء التنافسي دراسة تطبيقية في شركتي التأمين العراقية العامة والحمراء للتأمين الأهلية. رسالة ماجستير منشورة . كلية إدارة الأعمال ، جامعة بغداد. بغداد.
- البار، عدنان مصطفى. (2021). أمن المعلومات والأمن السيبراني . جدة: جامعة الملك عبد العزيز.
- حمدان، أحمد عبد الله. (2021). أمن وسرية المعلومات وأثرها في الأداء المصرفي: دراسة تطبيقية على البنوك العاملة في الأردن .رسالة ماجستير منشورة . كلية السلط التقنية ، جامعة البلقاء التطبيقية ، البلقاء.
- الخالدي ، ساري محمد . (2016). اتجاهات في أمن المعلومات وأمانها: أهمية تقنيات التعمية - التشفير. المنامة : أكاديمية الخليج العربي للدراسات .
- درويش، محمود أحمد. (2018). مناهج البحث في العلوم الإنسانية. الرياض: مكتبة ابن تيمية للنشر.
- الزهراني ، أحمد سعيد. (2018) آثار قرصنة البرمجيات عالميا. رسالة ماجستير منشورة. كلية العلوم الإستراتيجية. جامعة نايف العربية للعلوم الأمنية :الرياض
- السامي ، علاء الكيلاني . (2019). أساسيات نظم المعلومات الإدارية. مكتبة وائل: عمان.
- سكيكر ، محمد علي. (2022). الجريمة المعلوماتية و كيفية التصدي لها. ط2. الدار البيضاء : دار النشر المغربية .
- السهلي، فارس بن صالح. (2019). نطاق مسؤولية الناقل الجوي للركاب وأساسها في نظام الطيران المدني السعودي. الرياض: مطابع وزارة الداخلية.
- الشاربي، خالد جويش. (2017): الأمن السيبراني في المملكة العربية السعودية. الرياض: مكتبة دار القلم.
- الصيدلاني، خالد صالح. (2017). واقع قرصنة البرمجيات في الأردن وسبل مواجهتها. رسالة ماجستير منشورة . كلية الأعمال : الجامعة الأردنية.
- عبد ربه ، رائد محمد. (2020). مبادئ نظم المعلومات الإدارية. بيروت: مكتبة بيروت الحرة.
- عطوان، أسعد محمد. (2016). مناهج البحث العلمي. ط2. القاهرة: مكتبة دار المعارف.
- العضياني ، ماجد محمد . (2018). انتهاك خصوصية البيانات في مؤسسات الأعمال وأثره على أداء المؤسسات . رسالة ماجستير منشورة .كلية التجارة . القاهرة : جامعة القاهرة .
- الغامدي، محمد حسن. (2021). فرص حلول الأمن السيبراني في المملكة العربية السعودية . الرياض: مطابع فنتك السعودية.

- فايز ، وائل علي. (2019). دور تكنولوجيا المعلومات في تدعيم أداء الموارد البشرية (دراسة ميدانية).رسالة ماجستير منشورة . كلية التربية. المنصورة: جامعة المنصورة.
- القحطاني ، منصور سعيد. (2019). مهددات الأمن المعلوماتي وسبل مواجهتها.ط2. الرياض : مكتبة دار القلم .
- الكبيسي، حامد جهاد. (2019). مناهج البحث العلمي في العلوم الإدارية. الرياض: مكتبة العبيكان.
- موقع الهيئة العامة للطيران المدني بالمملكة العربية السعودية-<https://www.gaca.gov.sa/web/ar-sa/page/home>
- نوبي ، فاطمة إبراهيم. (2021). أثر كفاءة أداء الموارد البشرية على سلامة الطيران المدني بالتطبيق على قطاع الطيران المدني المصري. القاهرة : أكاديمية السادات.
- الهيئة الوطنية للأمن السيبراني. (2018). التعريف بالهيئة الوطنية للأمن السيبراني . الرياض : مطابع وزارة الداخلية.
- الهيئة الوطنية للأمن السيبراني. (2018). الضوابط الأساسية للأمن السيبراني في المملكة العربية السعودية . الرياض: مطابع وزارة الإعلام.
- الهيئة العامة للإحصاء. (2018). موجز إحصاءات هيئة الطيران المدني بالمملكة العربية السعودية. الرياض: مطابع الهيئة العامة للإحصاء.
- ياغي، محمد. (2017). الأمن المعلوماتي وإدارة العلاقات الدولية. عمان: دار وائل للنشر والتوزيع.

المراجع الأجنبية:

- Lipps, k (2020). Interest in organizing information technology courses, a new educational entrance in the European Union. Eric Digest. (110). Ed:823493.
- Lerner, G (2021). The role of information technology in the preparation of human competencies at the Center (Izonti). An Electronic Journal of the U.S. Department of Educational Sciences. from <http://usinfo.state.gov/journals>.
- Stephen, S. (2018). Reasons for individuals and organizations to violate the privacy of information, and the role of cyber security in the face of the phenomenon. Eric Digest . No.(284) . Ed:536981.
- Waldo, R. (2018). Cyber awareness of the privacy of information and data using web-based knowledge flights, a new educational portal in the European Union. Eric Digest .No.(263) . Ed:598680.

الملاحق

ملحق (1)

استبانة التطبيق

بسم الله الرحمن الرحيم
والصلاة والسلام على أشرف الخلق والمرسلين نبينا محمد الصادق الأمين وعلى آله وصحبه أجمعين

إلى الشركاء في النجاح
السلام عليكم ورحمة الله وبركاته أما بعد،

أتقدم بالشكر الجزيل سلفاً على تكريمكم بالاجابة على هذه الاستبانة، والتي تهدف إلى جمع البيانات لتخدم بحث التخرج لدرجة الماجستير تحت عنوان: (سبل مساعدة لادارة مخاطر الأمن السيبراني في الشركات السعودية التقنية بحسب تشريعات الهيئة الوطنية للأمن السيبراني).
كما آمل تفضلاً بأن تكون الاجابات دقيقة وموضوعية لمحاور الاستبانة وذلك لتحقيق الهدف المنشود منها، علماً بأن هذه البيانات ستستخدم فقط لغاية البحث العلمي .

نسأل الله لنا ولكم التوفيق والسداد
مع خالص التحية والتقدير

الجزء الأول (البيانات الأولية):

1- العمر من:

- ☐ 30 سنة فأقل
- ☐ 31 إلى 40 سنة
- ☐ 41 إلى 50 سنة
- ☐ 51 فأكثر

2- المؤهل العلمي:

- ☐ ثانوية عامة
- ☐ دبلوم عالي / متوسط
- ☐ بكالوريوس
- ☐ ماجستير
- ☐ دكتوراه

3- المستوى الوظيفي:

- ☐ مدير
- ☐ مشرف
- ☐ موظف

4- الخبرة العملية:

- ☐ 5 سنوات فأقل
- ☐ من 6 إلى 10 سنوات
- ☐ أكثر من 11 سنة

5- مجال العمل أو التخصص:

- ☐ التخصصات التقنية أو المعلوماتية
- ☐ تخصصات الأمن السيبراني
- ☐ تخصصات ادارة المخاطر
- ☐ أخرى :

الجزء الثاني (محاوِر الاستبانة (1/3):

أولاً: من اسباب مخاطر الأمن السيبراني في المملكة العربية السعودية
توضيح: الاختيار يكون بحسب درجة الموافقة مع الاسباب المذكورة

#	العبارة	درجة الموافقة			
		موافق بشدة	موافق	لا أعلم	غير موافق بشدة
1	هجمات القرصنة الإلكترونية ومحاولات اختراق الأنظمة السيبرانية والحصول على معلومات حساسة أو التلاعب بها				
2	سرقة المعلومات الحساسة والتجسس على الأنشطة الحكومية والخاصة				
3	التصيد الإلكتروني عبر الإنترنت مثل الرسائل الاحتيالية، وسرقة الحسابات البنكية				
4	الهجمات التي تستهدف إعاقة البنية التحتية السيبرانية للمملكة، مثل تعطيل خدمات الإنترنت				
5	الاختراقات السيبرانية أو الأمنية للمؤسسات الحكومية والشركات والتي تهدد سرية المعلومات والملكية الفكرية وسلامة الأنظمة				
6	تهديدات البرمجيات الخبيثة والفايروسات التي يتم استخدامها لاختراق الأنظمة وتدمير البيانات أو سرقتها				
7	انتهاكات الخصوصية وتسريب المعلومات الشخصية للأفراد				
8	الهجمات السيبرانية على البنية التحتية الحيوية مثل الشبكات الكهربائية والماء والنقل				
9	الاحتيال المصرفي وسرقة المعلومات المالية مما يتسبب في خسائر مالية كبيرة				
10	تهديدات الهجمات السيبرانية على البنية الحيوية الوطنية مثل القطاعات النفطية والنقل والصناعة				

الجزء الثاني (محاور الاستبانة (2/3):

ثانيًا: أهمية الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني

توضيح: الاختيار يكون بحسب درجة الموافقة مع الالتزام بالنسبة للجهة التي تعمل بها

#	العبارة	درجة الموافقة			
		موافق بشدة	موافق	لا أعلم	غير موافق بشدة
1	تعيين فريق متخصص في الأمن السيبراني				
2	اعداد تقارير دورية عن تقييمات الأمن السيبراني وتحديد نقاط الضعف وخطط المعالجة				
3	انشاء برنامج خاص بالتوعية بالأمن السيبراني، بالإضافة إلى الاستثمار في تدريب الموظفين حول قضايا الأمن السيبراني				
4	تحديد واعتماد وثيقة لسياسات واجراءات الأمن السيبراني ويتم تطبيقها بشكل منتظم				
5	العمل على اعداد وتقديم تقارير مفصلة عن الاستجابة للحوادث السيبرانية وتحليلها ومشاركتها مع أصحاب العلاقة				
6	العمل على المراجعات الدورية لتحقيق من الامتثال لتشريعات الهيئة الوطنية للأمن السيبراني				
7	التعاون مع القطاعات الخاصة والحكومية في المملكة لتبادل المعلومات والمنفعة لتعزيز الأمن السيبراني				
8	الاستثمار لتطوير تقنيات تعزيز الأمن السيبراني				
9	التعاون بشكل وثيق مع الهيئة الوطنية للأمن السيبراني في تنفيذ الضوابط والتشريعات الأمنية اللازمة				
10	توثيق واعتماد استراتيجية للأمن السيبراني تتضمن الأهداف والمبادرات والمشاريع الخاصة في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة				

الجزء الثاني (محاور الاستبانة (3/3):

ثالثاً: طرق تطوير ادارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني
توضيح: الاختيار يكون بحسب درجة الموافقة مع الطريقة

#	العبارة	درجة الموافقة			
		موافق بشدة	موافق	لا أعلم	غير موافق بشدة
1	تعزيز الوعي بأهمية الأمن السيبراني وتدريب الموظفين على المخاطر والتهديدات السيبرانية				
2	حوكمة الأمن السيبراني من خلال تطوير وانشاء سياسات واجراءات خاصة بالأمن السيبراني، بالإضافة إلى تحديد اطار عمل لادارة مخاطر الأمن السيبراني وضمان تطبيقهم بشكل فعال				
3	تعيين ذوي الخبرة لأعمال تحديد وتقييم المخاطر السيبرانية وتحليل الثغرات الأمنية في الأنظمة والشبكات والاشراف على تحقيق الامتثالات التشريعية للمشاريع التقنية				
4	تعيين فريق مختص للتعامل مع حوادث الأمن السيبراني والاستجابة السريعة لها				
5	تعزيز التعاون والتنسيق بين القطاعات العامة والخاصة والهيئات الأخرى في المملكة، بالإضافة إلى توسيع التعاون مع المنظمات الدولية الأمنية				
6	انشاء لجنة اشرافية متخصصة للأمن السيبراني لعرض ومناقشة الوضع السيبراني، وضمان مراجعة تطبيق المتطلبات التشريعية بشكل دوري وابداء الدعم اللازم				
7	تبني البحث والتطوير في مجال الأمن السيبراني ودعم الجهود التعليمية لتأهيل المتخصصين في هذا المجال				
8	مراجعة وتحديث التشريعات القائمة لتعزيز القدرة على مكافحة الجرائم السيبرانية ومخاطر الأمن السيبراني				
9	ضمان معالجة واغلاق الثغرات الأمنية بناءً على تصنيفها والمخاطر السيبرانية المترتبة عليها				
10	التواصل والاشتراك مع مصادر موثوقة فيما يتعلق بالتنبيهات الخاصة بالثغرات الجديدة والمحدثة، وتبليغ الهيئة الوطنية للأمن السيبراني عند حدوث حادثة أمن سيبراني				

ملحق (2)

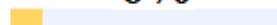
فحص نسبة الاقتباس



Plagiarism Checker X - Report

Originality Assessment

6%



Overall Similarity

Matches: 2967 / 24884 words
Sources: 51

Remarks: Low similarity detected, check with your supervisor if changes are required.

Midocean University

College of Management

Department of Risk Management

Title in English

Ways to help manage Cybersecurity Risks in Saudi IT Companies according to the legislation of
the National Cybersecurity Authority

Prepared by:

Hotaf Abdullah Khalil

Supervised by:

Dr. Walid Abdul Jawad Suliman Siddeq

Dr. Al-Faisal Abdulhamid Mohammed Hasan

Year:2023