

إدارة مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية –
بالتطبيق على وزارة الاتصالات وتقنية المعلومات.

إعداد الطالب/

إشراف/

العام الدراسي:

٢٠٢٤



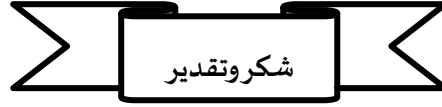
الإهداء

الى والدتي الغالية ... الى والدي الحبيب

الى من ساندني ومد يد العون لي ... زوجي الغالي

الى اساتذتي الافاضل

الى كل هؤلاء ... اهدي ثمرة جهدي المتواضع



أتوجه بالشكر والتقدير إلى كل من ساهم في مسيرتي التعليمية وساندني لإنجاز هذا العمل وأخص بالذكر الأستاذ الفاضل الدكتور / (.....) الذي أشرف على هذا البحث، والذي لم يبخل علي بمعلوماته وتوجيهاته السديدة لإخراج هذا البحث إلى حيز الوجود، وأحمد الله تعالى حمدا كثيرا طيبا على إتمام هذا البحث والله عز وجل أسأله التوفيق والسداد ولكم مني جميعا بالغ التقدير وعظيم الامتنان.

الباحث

ملخص البحث باللغة العربية

إدارة مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية -
بالتطبيق على وزارة الاتصالات وتقنية المعلومات.

هدفت الدراسة إلى التعرف على إدارة مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية - بالتطبيق على وزارة الاتصالات وتقنية المعلومات. وقد استخدمت الدراسة المنهج الوصفي التحليلي وأداة الاستبانة. وتمثل مجتمع الدراسة في منسوبي وزارة الاتصالات وتقنية المعلومات في منطقة الرياض والبالغ عددهم (٥٧٠) موظف وموظفة. وبلغت حجم عينة الدراسة (١٢٠) مفحوص من منسوبي وزارة الاتصالات وتقنية المعلومات في منطقة الرياض. وتم اختيار العينة بالطريقة العشوائية عن طريق وضع الأسماء على جهاز الحاسب الآلي والاختيار من بينها، وقام الباحث 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 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). ومن التوصيات التي وضعتها الدراسة : يجب أن تكون المؤسسات ملتزمة بتعزيز التوعية وتوفير التدريب المستمر للموظفين بشأن مخاطر الأمن السيبراني وأفضل الممارسات للوقاية منها. ينبغي تعزيز الوعي بحماية المعلومات الحساسة وتحذير الموظفين من التهديدات السيبرانية المحتملة مثل الهجمات الاجتماعية والبريد الإلكتروني الاحتيالي.

الكلمات المفتاحية:

إدارة/مخاطر الأمن السيبراني /المؤسسات /وزارة الاتصالات وتقنية المعلومات.

Abstract

Cybersecurity Risk Management in Government Institutions in the Kingdom of Saudi Arabia - Applied to the Ministry of Communications and Information Technology.

The study aimed to identify cybersecurity risk management in government institutions in the Kingdom of Saudi Arabia - Applied to the Ministry of Communications and Information Technology. The study used the descriptive analytical approach and the questionnaire tool. The study community represented the employees of the Ministry of Communications and Information Technology in the Riyadh region, numbering (570) male and female employees. The size of the study sample amounted to (120) examinees from the employees of the Ministry of Communications and Information Technology in the Riyadh region. The sample was selected randomly by putting names on the computer and choosing from among them, and the researcher designed an electronic questionnaire to achieve the objectives of the study. The study reached important results, including: The phrases of the axis of the importance of adhering to the legislation of the National Cybersecurity Authority came in at a (high) degree, as the overall arithmetic mean was (3.73 out of 5), which is an average that falls within the fourth category of the five-point Likert scale categories (3.40 to 4.19), which is the category that indicates a (high) degree. There is a disparity in the responses of the study sample members to the phrases of the axis of ways to develop cybersecurity risk management according to the legislation of the National Cybersecurity Authority, as the averages ranged between (3.52 to 3.86 out of 5), which are averages that fall within the fourth category of the five-point Likert scale categories and indicate a (high) degree. Among the recommendations set by the study: Institutions must be committed to enhancing awareness and providing continuous training for employees on cybersecurity risks and best practices for preventing them. Awareness should be enhanced to protect sensitive information and warn employees of potential cyber threats such as social attacks and fraudulent email.

key words:

Management / Cybersecurity Risks / Institutions / Ministry of Communications and Information Technology.

الموضوع	الصفحة
صفحة العنوان	-
صفحة البسملة	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	١
مقدمة الدراسة	١
مشكلة الدراسة	٢
أهمية الدراسة	٣
أهداف الدراسة	٥
أسئلة الدراسة	٥
الدراسات السابقة	٥

٩	المنطلقات النظرية للدراسة
١١	المنهجية وطرق البحث الأخرى
١٣	حدود البحث
١٤	الفصل الثاني: أدبيات الدراسة
١٤	١- مفهوم الأمن السيبراني
١٥	٢- أهمية الأمن السيبراني
١٦	٣- أهداف الأمن السيبراني
١٧	٤- العناصر الأساسية للأمن السيبراني :
٢٠	٥- عوامل تحقيق الأمن السيبراني
٢١	٦- مخاطر الأمن السيبراني
٢٤	٧- أهمية تشريعات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية
٢٥	٨- سبل تعزيز الأمن السيبراني في المملكة العربية السعودية :
٢٨	الفصل الثالث: إجراءات البحث (المنهجية والإجراءات)
٢٨	٣-١: منهج البحث
٢٨	٣-٢: مجتمع وعينة البحث
٢٩	٣-٣: أداة البحث
٣٠	٣-٤: صدق أداة البحث
٣١	٣-٥: ثبات أداة البحث
٣٣	٣-٦: الأساليب الإحصائية

٣٤	الفصل الرابع: نتائج الدراسة الميدانية
٣٤	١-٤: مقدمة:
٣٨	٢-٤: خصائص عينة الدراسة
٤١	٣-٤: نتائج الدراسة الميدانية
٤٨	الفصل الخامس: خلاصة لأهم نتائج الدراسة وتوصياتها
٤٨	١-٥: خلاصة الدراسة
٤٩	٢-٥: نتائج الدراسة
٥٠	٣-٥: توصيات الدراسة
٥٢	٤-٥: مقترحات الدراسة
٥٣	المراجع
٥٣	المراجع العربية
٥٥	المراجع الأجنبية
٥٦	الملاحق

الصفحة	الجدول	فهرس الجداول
٢٩	جدول رقم (٣-١) مقياس ليكرت الخماسي	
٣٠	جدول رقم (٣-٢) معاملات ارتباط بيرسون بين درجات كل فقرة والدرجة الكلية للبعد الذي تنتهي إليه.	
٣١	جدول رقم (٣-٣) معاملات الارتباط بين درجة كل بعد والدرجة الكلية للاستبانة.	
٣٢	جدول رقم (٣-٤) معاملات ثبات أداة الدراسة.	
٣٣	جدول (٣-٥) الوزن النسبي للدرجات.	
٣٣	جدول (٣-٦) المتوسط المرجح للدرجات	
٣٤	جدول (٤-١) توزيع عينة الدراسة حسب العمر	
٣٥	جدول (٤-٢) توزيع عينة الدراسة حسب المؤهل العلمي	
٣٦	جدول (٤-٣) توزيع عينة الدراسة حسب المستوى الوظيفي	
٣٧	جدول (٤-٤) توزيع عينة الدراسة حسب الخبرة العملية	
٣٨	جدول (٤-٥) توزيع عينة الدراسة حسب مجال العمل/ التخصص	
٣٩	جدول (٤-٦) المتوسطات الحسابية والانحرافات المعيارية لأبعاد إدارة مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية – بالتطبيق على وزارة الاتصالات وتقنية المعلومات.	
٤٠	جدول (٤-٧) المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات اسباب مخاطر الأمن السيبراني في المملكة العربية السعودية مرتبة تنازليا حسب المتوسطات الحسابية.	
٤٣	جدول (٤-٨) المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات أهمية الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني مرتبة تنازليا حسب المتوسطات الحسابية.	

٤٥	جدول (٩-٤) المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات طرق تطوير ادارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني مرتبة تنازليا حسب المتوسطات الحسابية.
----	--

	فهرس الأشكال
الصفحة	الشكل
٣٥	الشكل رقم (١) توزيع عينة الدراسة حسب العمر
٣٦	الشكل رقم (٢) توزيع عينة الدراسة حسب المؤهل العلمي
٣٦	الشكل رقم (٣) توزيع عينة الدراسة حسب المستوى الوظيفي
٣٧	الشكل رقم (٤) توزيع عينة الدراسة حسب الخبرة العملية
٣٨	الشكل رقم (٥) توزيع عينة الدراسة حسب مجال العمل

	فهرس الملاحق
الصفحة	الملحق
٥٧	ملحق (١) استبانة التطبيق
٦٣	ملحق (٢) فحص نسبة الاقتباس

الفصل الأول

خطة البحث

مقدمة الدراسة

إن تنوع وسائل الاتصالات وتفاوت خصائصها وطبيعتها زاد من حجم تبادل المعلومات بين العالم بشكل تسبب في زيادة العبء على الدول التي تسعى إلى تحقيق الأمن المطلوب للفرد والمجتمع في ظل الاستخدام الواسع للحاسب الآلي وتطبيقاته، والأجهزة الذكية، وكذلك ما يندرج تحتها ، ولقد شكل الأمن على مر التاريخ الهاجس الأكبر للدول التي اعتبرت ضمان بقائها واستمرارها من بين أولويات سياستها ، فالأمن هدف تسعى إليه كل الدول كونه أحد أهم مقومات الحياة الإنسانية ، أمام هذا الاحتياج الملح يبرز دور الأفراد والدولة ، المؤسسات و المنظمات الإقليمية والعالمية في العملية الأمنية (الخالدي، ٢٠١٦، ص ٥٢-٥٣).

إن تشريعات الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية تهدف إلى تعزيز وتعزيز أمان البنية التحتية السيبرانية في المملكة وحماية المعلومات الحساسة والتحقق من سلامة البيانات المتداولة. ويتعين على المنظمات تحديد وتحليل المخاطر المحتملة للأمن البيانات والأنظمة السيبرانية الخاصة بها. (الغامدي، ٢٠٢١، ص ١٧).

ويتطلب ذلك تقييم وتحليل التهديدات المحتملة وثغرات الأمان وتأثيرها المحتمل على المنظمة. كما يجب على المنظمات تنفيذ إجراءات أمنية فعالة لحماية الأنظمة والبيانات الحساسة من التهديدات السيبرانية. ويشمل ذلك تطبيق سياسات الأمان والوصول والتحقق من الهوية وتحديث البرامج والأجهزة وتأمين الشبكات والتدريب على الوعي الأمني . ونظرا لأهمية الأمن المعلوماتي في العصر الحديث ، فقد صدر أمر ملكي كريم بإنشاء هيئة باسم الهيئة الوطنية للأمن السيبراني، ترتبط بمقام خادم الحرمين الشريفين، وتضع الهيئة في أولوياتها استقطاب الكوادر الوطنية المؤهلة والطموحة وتأهيلها وتمكينها ، وبناء الشراكات مع الجهات العامة والخاصة، وتحفيز الابتكار والاستثمار في مجال الأمن السيبراني للإسهام في تحقيق نهضة تقنية تخدم مستقبل الاقتصاد الوطني للمملكة. وتهدف الهيئة إلى تعزيز حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات، وما تحويه من بيانات، مراعية في ذلك الأهمية الحيوية المتزايدة للأمن السيبراني في حياة المجتمعات،

ومستهدفة التأسيس لصناعة وطنية في مجال الأمن السيبراني تحقق للمملكة الريادة في هذا المجال انطلاقاً مما تضمنته رؤية المملكة العربية السعودية ٢٠٣٠ (الهيئة الوطنية للأمن السيبراني ، ٢٠١٨ ، ص ٩٦-٩٧).

ويمثل الأمن الوطني أحد المقومات الأساسية لنجاح عملية التنمية، والنمو، والارتقاء بمختلف المجالات؛ حيث يعد الإبداع الفكري، والذهني، والتخطيط المنظم، والسليم، والمثابرة العلمية، من أهم مرتكزات التنمية، ولا يتحقق ازدهار لمشروع التنمية إلا في ظل وجود أمن راسخ يدعم، ويتيح وجود هذه المرتكزات، مما يمكن الإنسان من الاطمئنان على ذاته، وثروته، واستثماراته (الشراري، ٢٠١٧، ص ٨٨).

يتضح مما سبق أنه يجب على المنظمات وضع خطط استجابة للحوادث الأمنية وتنفيذها عند حدوث أي انتهاك أمني. ويشمل ذلك التعامل مع الاختراقات والتهديدات المحتملة واستعادة الأنظمة وتحليل الحوادث لتعزيز الأمان في المستقبل. وتشترط تشريعات الهيئة الوطنية للأمن السيبراني الامتثال للمعايير والإرشادات الأمنية المعترف بها عالمياً. يجب على المنظمات مراجعة سياساتها وإجراءاتها للتأكد من الامتثال لهذه المعايير والإشعار بأي انتهاكات أمنية محتملة. ويتناول الباحث في تلك الدراسة موضوع إدارة مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية - بالتطبيق على وزارة الاتصالات وتقنية المعلومات.

مشكلة الدراسة

تتمثل مشكلة الدراسة الحالية في أنه يجب على المنظمات تعزيز التوعية الأمنية لدى الموظفين وتوفير التدريب المناسب لهم بشأن مخاطر الأمن السيبراني وكيفية التعامل معها. يمكن أن يشمل ذلك التعريف بالتهديدات السيبرانية المحتملة وطرق الوقاية منها والإبلاغ عن أي حالات انتهاك أمني. كما يجب على المنظمات إجراء تقييم دوري لامتثالها لتشريعات الهيئة الوطنية للأمن السيبراني والمعايير الأمنية المعمول بها. يشمل ذلك تنفيذ عمليات التدقيق الداخلي والتقييم الخارجي للتأكد من مستوى الامتثال وتحديد أي نقاط ضعف 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، وأيضا حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به

لأهداف غير سليمة، وهو السبب وراء الأمر الملكي بإنشاء الهيئة الوطنية للأمن السيبراني (الخالدي، ٢٠١٦، ص ٤١).

وينتهج الأمن السيبراني الناجح نهجا معيناً يتكون عادة من طبقات متعددة للحماية تنتشر في أجهزة الكمبيوتر أو الشبكات أو البرامج أو البيانات التي ينوي المرء الحفاظ على سلامتها و في أي منظمة يجب على المستخدمين والعمليات وكذلك التكنولوجيا أن يكملوا بعضهم بعضاً ويتكاتفوا لإنشاء دفاع فعال من الهجمات السيبرانية (عبد ربه ، ٢٠٢٠ ، ص ٦٣).

وقد أكدت نتائج دراسة والدو (Waldo ، ٢٠١٧، ص ١٣) 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 النسخ الاحتياطي للبيانات .

يتضح مما سبق أنه من الضروري التعاون مع الهيئة الوطنية للأمن السيبراني ومشاركة المعلومات الأمنية الحيوية معها. يساهم التعاون في تعزيز القدرة على التصدي للتهديدات السيبرانية وتعزيز الأمان السيبراني على المستوى الوطني. وتشجع 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: ما سبل إدارة مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية ؟

أهمية الدراسة

تتضح أهمية الدراسة ، فيما يلي:

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 في البلد المعين وكيفية تطبيقه لإدارة مخاطر الأمن السيبراني.

- 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 الأمان 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 للتهديدات السيبرانية.

- يساعد البحث على فهم متطلبات الامتثال لتشريعات الهيئة الوطنية للأمن السيبراني. ويمكن للمؤسسات والشركات أن تستفيد من هذا البحث للامتثال القانوني 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 للمؤسسات والأفراد فيما يتعلق بالأمن السيبراني. ومن خلال فهم تشريعات الهيئة الوطنية للأمن السيبراني وتطبيقها، يمكن للمؤسسات تحديد مسؤولياتها واتخاذ الإجراءات اللازمة للحماية من التهديدات السيبرانية وتفادي المسائل القانونية.

أهداف الدراسة

تهدف تلك الدراسة إلى ما يلي:

١. التعرف على مخاطر الأمن السيبراني في المملكة العربية السعودية
٢. التعرف على مدى الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية.
٣. التعرف على سبل تطوير دور إدارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني.

أسئلة الدراسة

- تتمثل مشكلة الدراسة في السؤال الرئيس التالي : ما سبل ادارة مخاطر الأمن السيبراني بحسب تشريعات الهيئة الوطنية للأمن السيبراني؟
- ويتفرع من التساؤل الرئيس السابق التساؤلات الفرعية التالية:
١. ما مخاطر الأمن السيبراني في المملكة العربية السعودية؟
 ٢. ما مدى الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية؟
 ٣. ما سبل تطوير دور إدارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني ؟

الدراسات السابقة والإطار النظري.

أولاً: الدراسات السابقة

نتناول الدراسات السابقة مرتبة من الأقدم إلى الأحدث ، كما يلي :

دراسة الصيدلاني (٢٠١٧) 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 ١٢٠ من موظفي (١١) شركة خدمية بمدينة عمان العاصمة، وقد استخدمت الدراسة المنهج الوصفي التحليلي ، وتمثلت 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 (٢٠١٧) 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 (١٢٤) من خبراء تكنولوجيا المعلومات بمؤسسة جون بريد بضاحية لندن الغربية بالمملكة المتحدة. وقد توصلت الدراسة إلي 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.

ودراسة والدو Waldo (٢٠١٨) بعنوان : التوعية السيبرانية بخصوصية المعلومات والبيانات باستخدام الرحلات المعرفية عبر الويب ، مدخل تعليمي جديد في الاتحاد الأوروبي . هدفت الدراسة إلي توجيه نظر القائمين على السياسة الأمنية في الاتحاد الأوروبي إلي 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 (٧) جامعات ومعاهد علمية في بلجيكا وبريطانيا وهولندا . وقد توصلت الدراسة إلي 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.

ودراسة الزهراني (٢٠١٨) بعنوان : آثار قرصنة البرمجيات عالميا ، وتمثل هدف الدراسة في التعرف على آثار قرصنة البرمجيات عالميا . وقد استخدمت الدراسة المنهج الوصفي التحليلي . وطبقت الدراسة على (٧٩) من خبراء تكنولوجيا المعلومات بجامعة القاهرة . وتم 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 .

و دراسة العضوياني (٢٠١٨) بعنوان : انتهاك خصوصية البيانات في مؤسسات الأعمال وأثره على أداء المؤسسات . و تمثلت 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 ١٣٢ 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.

و دراسة فايز (٢٠١٩) 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 (١١٨) من العاملين بشركة جهيئة بمصر . وقد توصلت الدراسة إلى نتائج هامة ومنها : أن تكنولوجيا المعلومات تعمل على تطوير أداء الموارد البشرية بالشركة ، و أبدى أغلبية عينة الدراسة (٩٨% منهم) شعورهم الإيجابي بأهمية التدريب .

و دراسة إبداح (٢٠١٩) 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 (٧٠) 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 .

و دراسة ليبس Lipps (٢٠٢٠) 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 الإتحاد . وقد استخدم الباحث المنهج المسحي وأداة الإستبانة . وقد طبق الباحث دراسته على (٧) 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.

ودراسة حمدان (٢٠٢١) 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 ٥٠% من مجتمع الدراسة (٦١٥) 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 (٤.١١). كما تبين أن الأهمية النسبية للأداء المصرفي في البنوك العاملة في الأردن كانت مرتفعة، إذ بلغ المتوسط الحسابي (٤.٠٧) 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.

ودراسة لينر Lerner (٢٠٢١) بعنوان : "دور تكنولوجيا المعلومات في إعداد الكفاءات البشرية بمركز (ايزونتي) " : هدفت الدراسة إلى عرض تجربة مركز (ايزونتي للصحة النفسية) بمدينة (أنتويرب) ببلجيكا في إعداد الكفاءات البشرية. وطبقت الدراسة على عدد (٢٦) 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 الدراسات السابقة:

بعد استعراض الدراسات السابقة تبين ما يلي:

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 وأيضاً اختلاف الفترة الزمنية التي سوف تتم فيها الدراسة الحالية عن الفترات الزمنية التي تمت فيها الدراسات السابقة . وسوف نستفيد من الدراسات السابقة فيما يلي :

- التأصيل النظري للدراسة الحالية
- في تحديد مصطلحات الدراسة
- في الاطلاع على دراسات سابقة في موضوع الدراسة الحالية
- في الاستفادة من الدراسات السابقة في تحديد منهج الدراسة
- في بناء أداة الدراسة
- تحديد الأساليب الإحصائية المناسبة
- في تحليل وتفسير النتائج التي توصلت إليها الدراسة.

المنطلقات النظرية للدراسة

تتمثل النظريات المفسرة لإدارة مخاطر الأمن السيبراني ، فيما يلي :

- ١-نظرية النموذج الدائري للأمن السيبراني (Cybersecurity Diamond Model): تعتبر هذه النظرية منهجاً شاملاً لفهم وتحليل مخاطر الأمن السيبراني. وتتألف النظرية من أربعة عناصر رئيسية هي: المهاجم (Adversary)، والضحية (Victim)، والسلوك (Behavior)، والتهديدات والضعف (Threats and Weaknesses). وتعزز هذه النظرية فهم كيفية تفاعل هذه العناصر وتوفير إطاراً لتحليل المخاطر وتصميم استراتيجيات الحماية.
- ٢-نظرية الانحدار العقدي 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 هجمات سيبرانية. وتساعد هذه النظرية المؤسسات على تحديد نقاط الضعف وتحسين قدراتها في مجال الأمان السيبراني.

٣-نظرية السلسلة الإمدادية للأمان السيبراني (Cybersecurity Supply Chain):

تركز هذه النظرية على أهمية حماية سلسلة الإمداد التكنولوجي والتأكد من أمان الموردين والجهات الفاعلة الأخرى في البيئة السيبرانية. وتعتبر هذه النظرية مهمة في تقييم المخاطر المحتملة التي يمكن أن تنشأ عند التعامل مع جهات خارجية (فايز، ٢٠١٩، ص ٤٥-٤٧).

٤-نظرية السلوك البشري في الأمن السيبراني (Human Behavior in Cybersecurity):

تركز هذه النظرية على الجانب البشري في أمن المعلومات والأمان 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.

٥-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 للمؤسسات تحديد الثغرات الأمنية المحتملة واتخاذ التدابير الوقائية المناسبة.

٦-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.

٧-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 الإرشادات اللازمة للمؤسسات للتعامل مع الحوادث السيبرانية بشكل منهجي وفعال.

٨-نظرية السلوك البشري في الأمن السيبراني (Human Behavior Theory in Cybersecurity):

تركز هذه النظرية على فهم سلوك المستخدمين ودورهم في تعزيز الأمن السيبراني أو تعريضه للمخاطر. وتهدف النظرية إلى تحليل العوامل النفسية والسلوكية التي تؤثر في قرارات المستخدمين المتعلقة بالأمن السيبراني، مثل التصرفات السلوكية الخاطئة أو الاستخدام السليم لكلمات المرور (سكيكر، ٢٠٢٢، ص ١١٣-١١٥).

ويتبنى الباحث في تلك الدراسة نظرية السلوك البشري في الأمن السيبراني، حيث أن نظرية السلوك البشري تعتبر أحد الجوانب الهامة في مجال الأمن السيبراني. ففي سياق الأمن السيبراني، يتعامل المختصون مع الجوانب التقنية والتحديات الفنية، ولكن يجب أيضا أن يأخذوا في الاعتبار الجانب البشري. فالبشر يشكلون جزءا أساسيا في أنظمة الأمان وقد يكونون عرضة للهجمات السيبرانية أو قد يسببون تهديدا غير مقصود للأمن.

المنهجية وطرق البحث

منهج الدراسة

سوف نتبع في هذه الدراسة المنهج الوصفي التحليلي ، إذ يختص بوصف الواقع من أجل فهمه وكيفية التعامل معه فهو تمهيد منطقي لوصف واقع الأشياء.

مجتمع وعينة البحث

سوف يتحدد مجتمع الدراسة في منسوبي وزارة الاتصالات وتقنية المعلومات والبالغ عددهم (٥٧٠) موظف وموظفة (الهيئة العامة للإحصاء، ١٤٤٤ ، ص ٩٦).

وسوف يتم اختيار نسبة لا تقل عن ٢٠% من منسوبي وزارة الاتصالات وتقنية المعلومات. وسوف يتم اختيار العينة بالطريقة العشوائية عن طريق وضع الأسماء على جهاز الحاسب الآلي والاختيار من بينها.

وسوف تتكون هذه الدراسة، مما يلي:

الفصل الأول: مقدمة البحث.

الفصل الثاني: الإطار النظري

الفصل الثالث: إجراءات البحث (المنهجية والإجراءات)

الفصل الرابع: الدراسة الميدانية وتحليل ومناقشة النتائج.

الفصل الخامس: خلاصة لأهم نتائج الدراسة وتوصياتها

المصادر والمراجع، ثم الملاحق.

أدوات البحث (أدوات جمع البيانات).

أداة البحث

سوف نقوم بتصميم إستبانة من خلال النظر إلى الأدبيات والدراسات السابقة ، وسوف تتكون أداة الدراسة من قسمين، نوضحها كما يلي:

القسم الأول: البيانات الشخصية.

القسم الثاني: محاور الاستبانة.

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

جدول رقم (١)

مقياس ليكرت الخماسي

المعيار	موافق بشدة	موافق	إلى حد ما	غير موافق	غير موافق بشدة
الدرجة	5	4	3	2	1
المتوسط الحسابي	٥.٠٠-٤.٢٠	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

حدود البحث

تحدد الدراسة الحالية بالحدود التالية:

■ الحدود الموضوعية:

سوف تركز الدراسة على إدارة مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية – بالتطبيق على وزارة الاتصالات وتقنية المعلومات.

■ الحدود البشرية:

منسوبي وزارة الاتصالات وتقنية المعلومات.

■ الحدود المكانية:

منطقة الرياض.

■ الحدود الزمنية:

سوف تجري الدراسة خلال العام ١٤٤٦هـ/٢٠٢٤م.

الفصل الثاني

أدبيات الدراسة

١- 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. والأمن السيبراني هو سلاح استراتيجي بيد الحكومات والأفراد لا سيما أن الحرب السيبرانية أصبحت جزءاً لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول. وينتهج الأمن السيبراني الناجح نهجاً معيناً يتكون عادة من طبقات متعددة للحماية تنتشر في أجهزة الكمبيوتر أو الشبكات أو البرامج أو البيانات التي ينوي المرء الحفاظ على سلامتها و في 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، وأيضاً حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به لأهداف غير سليمة، وهو السبب وراء الأمر الملكي بإنشاء الهيئة الوطنية للأمن السيبراني (الشراري ، ٢٠١٧، ص٣٩-٤٠).

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 ضرراً دائماً. وهذا يتمثل في تقليل احتمالات تجسد أي تهديد، والحد من الضرر الناجم أو سوء الأداء، وضمان استعادة العمليات العادية لحالتها السابقة خلال إطار زمني مقبول وبتكلفة مقبولة في أعقاب وقوع حادث أمني. 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 ويعتق 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 تشمل 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، كسر 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، ٢٠١٩، ص ١١-١٣).

٢- أهمية الأمن السيبراني

تحدد أهمية الأمن السيبراني، فيما يلي:

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

٢. 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.

٣. 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 تعطّلها أو تعرضها للهجمات التي يمكن أن تتسبب في فوضى وتوقف الخدمات الحيوية (الزهراني، ٢٠١٨، ص ٤٧-٤٩).

٤. 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.

٥. 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.

٦. 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، ٢٠١٧، ص ٩٥-٩٧).

٣-أهداف الأمن السيبراني

تحدد أهداف الأمن السيبراني ، فيما يلي:

١. 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.

٢. 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.

٣. 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.

٤. 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.

٥. 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، ٢٠١٩، ص ٦٣-٦٥).

٤-العناصر الأساسية للأمن السيبراني :

تحدد العناصر الأساسية للأمن السيبراني ، فيما يلي :

أ. 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 .

ب. 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 لتقليل 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 و السلوكية للأفراد العاملين من وقت لآخر و ربما يتم تغيير مواقع عملهم و محاولة عدم احتكار المهام على موظفين محددين (سكيكر ، ٢٠١٠ ، ص ٤٩-٥١).

ج. 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 و العوائق 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 (السالحي ، ٢٠١٩ ، ص ١٢٥-١٢٧).

د. 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 المسؤولة 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 المجففات و ربطها بخطوط الاتصال و التي هي عبارة عن استخدام الخوارزميات الرياضية أو أجهزة و معدات لغرض تجفير تناقل المعلومات (عبد ربه ، ٢٠١٣ ، ص ٦٠-٦١).

هـ. 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 ، ٢٠١٩ ، ص ١٣٣).

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 تُخَلَقُ بها المعارف وبها يتم تقاسمها، فيمكن اعتبارها منبعاً للابتكار في المستقبل لا ينبغي استبعاد البلدان النامية عنه. فثورة 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، ٢٠١٨، ص ٢٥-٢٧).

٥-عوامل تحقيق الأمن السيبراني

هناك ثلاثة عوامل أساسية لتحقيق الأمن السيبراني وهي :

١- السرية : وتعني ما يلي :

- التحقق من شخصية المستخدم.

- تشفير الاتصالات وكلمات السر.

٢-السلامة : وتعني ما يلي :

- إجراء النسخ الاحتياطي الدوري بشكل منتظم.

- الفحص المستمر لضمان أمن الشبكات.

٣-التوفر: وتعني ما يلي :

- العمل على منع التعرض لهجمات حجب الخدمة.

- توفير اتصالات وشبكات احتياطية (الخالدي ، ٢٠١٦، ص٩٣-٩٥).

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 تَجِبُ 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، ٢٠٢١، ص ١٣-١٥).

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 تتزايد 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، وعمليات الإنتاج، وعمليات 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، ٢٠١٨، ص ١٩-٢٠).

٦- 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 الأسعى 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 ، و قد يصعب أحيانا التنبؤ بالدوافع العديدة للأشخاص الذين يقومون بها ، أما البعض الآخر فقد يكون غير مقصود كالأخطاء البشرية و الكوارث الطبيعية (الغامدي، ٢٠٢١، ص١٠٣-١٠٥).

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

أ . 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 ، و تشكل هذه الأخطاء الغالبية العظمى للمشاكل المتعلقة بأمن و سلامة نظم المعلومات في المنظمات (القحطاني ، ٢٠١٩ ، ص٢٩).

ب . الأخطار البيئية :

و هذه 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 نسبيا لإجراء الإصلاحات اللازمة و استرداد البرمجيات و قواعد البيانات (ياغي ، ٢٠١٧ ، ص٣٢).

ج . الجرائم الإلكترونية :

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

١. الجريمة المادية :

وهي التي تسبب أضرار مالية على المستهدف مثل :

- عملية السطو الإلكتروني 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 ، ٢٠١٧ ، ص٣٦-٣٧).

٢. الجريمة الثقافية :

وهي جرائم تتعلق بحقوق الملكية الفكرية لبرامج الكمبيوتر وكذلك سرقة بعض المعلومات المهمة والأفكار من أجهزة الضحايا ونسبها إليهم (ياغي ، ٢٠١٧ ، ص٤٧).

٣. الجريمة السياسية والاقتصادية :

وتتضمن ، ما يلي :

- نشر وإصدار إشاعات على مواقع ومراكز مهمة لكي تعطل مصالح الشعب.
- نشر السلوك الخاطئ بين الشباب كالإرهاب وإدمان الخمر والمخدرات حتى يفسدون المجتمع والشباب وذلك ليضرون الدولة لأسباب سياسية واقتصادية (السالمي ، ٢٠١٩ ، ص٥٢-٥٤).

٤. الجريمة الجنسية :

وتتضمن ، ما يلي :

- التغير 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 ، ٢٠١٩ ، ص٥٨).

٧-أهمية تشريعات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية

تحدد أهمية تشريعات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية ، فيما يلي:

١. 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.
٢. مكافحة التهديدات السيبرانية: تلعب تشريعات الهيئة الوطنية للأمن السيبراني دورا هاما 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.
٣. 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.
٤. 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.
٥. تعزيز الثقة الرقمية: تساهم 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.

ويرى الباحث 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، ٢٠١٨، ص ٨٩-٩١).

٨- سبل تعزيز الأمن السيبراني في المملكة العربية السعودية :

تحدد سبل تعزيز الأمن السيبراني في المملكة العربية السعودية ، فيما يلي :

١ - على مستوى الإدارة :

على الإدارات العامة والخاصة توحيد جهودها بهدف:

- وضع إستراتيجية وطنية لأمن الفضاء السيبراني.
- وضع أسس تعاون وطني بين الحكومة والقطاع العام والخاص.
- خلق القدرات الوطنية لإدارة الحوادث عبر إنشاء مركز وطني للاستجابة لحوادث الحاسب الآلي للمواجهة المخاطر.
- إنشاء مركز الاستجابة لطوارئ الحاسب الآلي .
- نشر ثقافة وطنية تعنى بأمن الفضاء السيبراني.
- حماية الفضاء الإلكتروني الحكومي.
- التنسيق والتعاون مع الجهات الإقليمية والدولية (القحطاني ، ٢٠١٩ ، ص ٤٧-٤٩).

٢ - على مستوى المؤسسات والشركات

يجب على المؤسسات والشركات المختلفة العمل على:

- منح أولوية أكبر للتدابير القانونية والأمنية ضمن عملياتهم الإلكترونية.

- ضمان الموارد الضرورية المخصصة لتخطيط واعتماد أنظمة حماية متعددة الطبقات لردع المخاطر عن أنظمة المعلومات والبنى التحتية التابعة لهم.
- تنفيذ وتطبيق عمليات وإجراءات أمنية واعتبارها مهمة إلزامية ذات أولوية هامة (القحطاني ، ٢٠١٩ ، ص ٥٥-٥٦).

٣ - على مستوى الجامعات والتعليم الأكاديمي

للجامعات دور أساسي في تأمين الدعم الأكاديمي المطلوب لتحفيز علم الأمن السيبراني عبر:

- إجراء بحوث لأكاديمية 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، ٢٠١٦، ص ١٥٩).

٤ - على مستوى 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 ، ٢٠١٦ ، ص ١١٤).

وهناك العديد من أنواع التدابير التي ينبغي توطيدها لزيادة أمن البنية التحتية للاتصالات وتكنولوجيا المعلومات. ومن بين هذه التدابير:

- 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، وبروتوكولات التشفير والإدارة التشغيلية (الغامدي، ٢٠٢١، ص ٥٨-٦٠).

وينبغي أن تستهدف استراتيجيات 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، ٢٠١٩، ص ١٧٦-١٧٨).

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

الفصل الثالث

إجراءات البحث (المنهجية والإجراءات)

١-٣: منهج البحث

اعتمدت الدراسة 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 وفقا لشواهد وقرائن متنوعة.

٢-٣: مجتمع وعينة البحث

تمثل مجتمع الدراسة في منسوبي على وزارة الاتصالات وتقنية المعلومات في منطقة الرياض والبالغ عددهم (٥٧٠) موظف وموظفة (الهيئة العامة للإحصاء، ١٤٤٤، ص ٩٦).

وبلغت حجم عينة الدراسة (١٢٠) مفرحوص من منسوبي وزارة الاتصالات وتقنية المعلومات في منطقة الرياض. وتم اختيار العينة بالطريقة العشوائية عن طريق وضع الأسماء على جهاز الحاسب الآلي والاختيار من بينها، وقام الباحث بتصميم إستبانة إلكترونية لتحقيق أهداف الدراسة.

٣-٣: أداة البحث

قام الباحث 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، وهي:

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

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

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

جدول رقم (٣-١)

مقياس ليكرت الخماسي

المعيار	موافق بشدة	موافق	إلى حد ما	غير موافق	غير موافق بشدة
الدرجة	5	4	3	2	1
المتوسط الحسابي	٥.٠٠-٤.٢٠	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

٤-٣: صدق أداة البحث

اعتمد الباحث 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 تنتمي 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 تنتمي إليه كما توضح نتائجها الجدول التالي:

جدول رقم (٢-٣) معاملات ارتباط بيرسون بين درجات كل فقرة والدرجة الكلية للبعد الذي تنتمي 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

*0.952	5	*0.835	5	*0.626	5
*0.916	6	*0.960	6	*0.707	6
*0.973	7	*0.949	7	*0.766	7
*0.965	8	*0.960	8	*0.949	8
*0.938	9	*0.966	9	*0.964	9
*0.986	10	*0.955	10	*0.958	10

* وجود دلالة عند مستوى (0.05)

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

جدول رقم (٣-٣) معاملات الارتباط بين درجة كل بعد والدرجة الكلية للاستبانة.

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

* 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 دالة إحصائياً عند مستوى دلالة (0.05) مما يعني وجود درجة عالية من الصدق البنائي للاستبانة.

٣-٥: ثبات أداة البحث

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

جدول رقم (٣-٤) معاملات ثبات أداة الدِّراسة.

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

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).

٦-٣: الأساليب الإحصائية

استخدم الباحث برنامج التحليل الإحصائي (Statistical Package for the Social Sciences) (SPSS)، حيث استخدمت الدراسة الأساليب الإحصائية التالية لاستخراج النتائج:

١. 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 الدِّراسة 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 الدِّراسة بالنسبة للمعلومات الأولية.

- المتوسط الحسابي وذلك لحساب المتوسط الحسابي لكل فقرة ولكل بعد.

- الانحرافات المعيارية للتعرف على التباين للفقرات وللأبعاد.

- معادلة المدى لمقياس ليكارت الخماسي لتحديد الدرجة ، كما في الجدول التالي:

جدول (٣-٥) 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 (٣-٦) المتوسط المرجح للدرجات

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

الفصل الرابع

نتائج الدراسة الميدانية

٤-١: مقدمة:

هدف البحث إلى التعرف على إدارة مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية – بالتطبيق على وزارة الاتصالات وتقنية المعلومات، ولبحث تساؤلات البحث تم بناء استبانة شملت هذه المتغيرات، وتم تطبيقها على أفراد عينة الدراسة البالغ عددهم (١٢٠) مفحوص من منسوبي وزارة الاتصالات وتقنية المعلومات في منطقة الرياض، وتم اختيار العينة بالطريقة العشوائية، وقام الباحث بتصميم إستبانة إلكترونية لتحقيق أهداف الدراسة. وقد تم إدخال البيانات إلى جهاز الحاسب الآلي وباستخدام البرنامج الإحصائي SPSS تم تحليل النتائج.

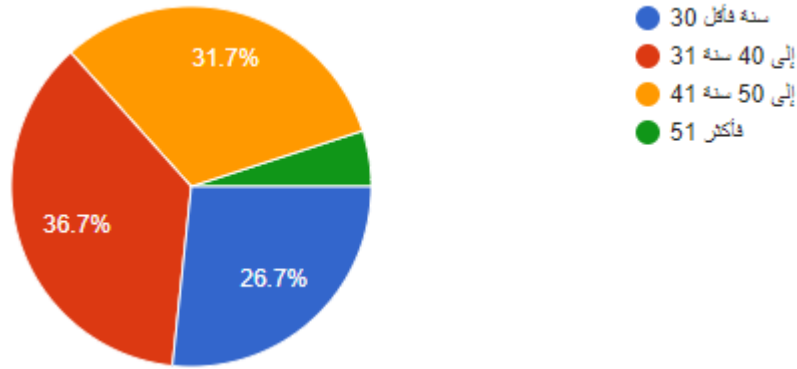
٤-٢: خصائص عينة الدراسة

١- حسب العمر

جدول (٤-١) توزيع عينة الدراسة حسب العمر

العمر	التكرار	النسبة
٣٠ سنة فأقل	٣٢	%٢٦.٧
٣١-٤٠	٤٤	%٣٦.٧
٤١-٥٠	٣٨	%٣١.٧
٥١ فأكثر	٦	%٥
المجموع	١٢٠	%١٠٠

يتضح من الجدول السابق أن أعلى نسبة في توزيع عينة الدراسة حسب العمر، هي: ٣١-٤٠ بنسبة %٣٦.٧، ثم ٣١-٤٠ بنسبة %٣٦.٧، ثم ٣٠ سنة فأقل بنسبة %٢٦.٧، ثم ٥١ فأكثر بنسبة %٥. كما يوضح الشكل التالي:



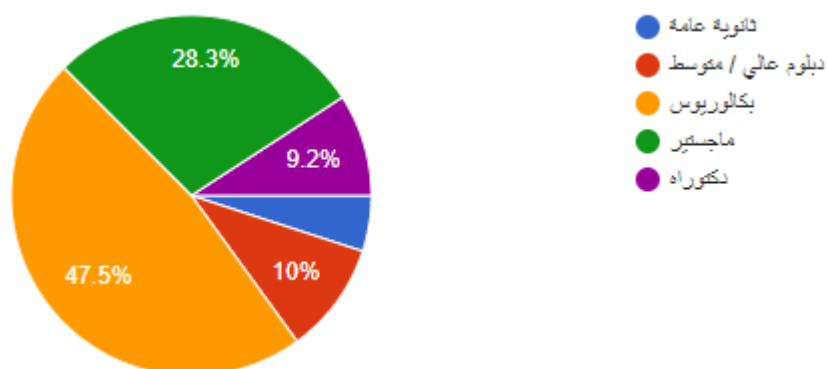
الشكل رقم (١) توزيع عينة الدراسة حسب العمر

٢- حسب المؤهل العلمي

جدول (٢-٤) توزيع عينة الدراسة حسب المؤهل العلمي

النسبة	التكرار	المؤهل العلمي
٥%	٦	ثانوية عامة
١٠%	١٢	دبلوم عالي/ متوسط
٤٧.٥%	٥٧	بكالوريوس
٢٨.٣%	٣٤	ماجستير
٩.٢%	١١	دكتوراه
١٠٠%	١٢٠	المجموع

يتضح من الجدول السابق أن أعلى نسبة في توزيع عينة الدراسة حسب الخبرة هي : بكالوريوس بنسبة ٤٧.٥%، ثم ماجستير بنسبة ٢٨.٥%، ثم دبلوم عالي/ متوسط بنسبة ١٠%، ثم دكتوراه بنسبة ٩.٢%، ثم ثانوية عامة بنسبة ٥%. ويتضح ذلك من الشكل التالي:



الشكل رقم (٢) توزيع عينة الدراسة حسب المؤهل العلمي

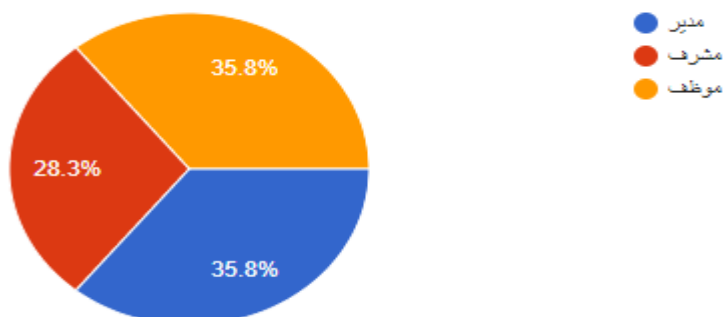
٣- حسب المستوى الوظيفي

جدول (٣-٤) توزيع عينة الدراسة حسب المستوى الوظيفي

المستوى الوظيفي	التكرار	النسبة
مدير	٤٣	٣٥.٨%
مشرف	٣٤	٢٨.٣%
موظف	٤٣	٣٥.٨%
المجموع	١٢٠	١٠٠%

يتضح من الجدول السابق أن أعلى نسبة في توزيع عينة الدراسة حسب المستوى الوظيفي هي: مدير وموظف بنسبة ٣٥.٨% لكل منهما ثم مشرف بنسبة ٢٨.٣%. ويتضح ذلك من

الشكل التالي:



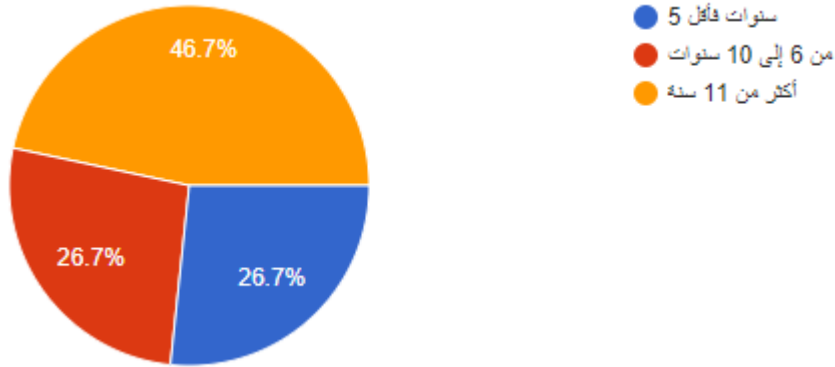
الشكل رقم (٣) توزيع عينة الدراسة حسب المستوى الوظيفي

٤- حسب الخبرة العملية

جدول (٤-٤) توزيع عينة الدراسة حسب الخبرة العملية

الخبرة العملية	التكرار	النسبة
٥ سنوات فأقل	٣٢	%٢٦.٧
١٠-٦	٣٢	%٢٦.٧
أكثر من ١١ سنة	٥٦	%٤٦.٧
المجموع	١٢٠	%١٠٠

يتضح من الجدول السابق أن أعلى نسبة في توزيع عينة الدراسة حسب الخبرة العملية هي: أكثر من ١١ سنة بنسبة %٤٦.٧، ثم ٥ سنوات فأقل ، و١٠-٦ بنسبة %٢٦.٧ لكل منهما. ويتضح ذلك من الشكل التالي:



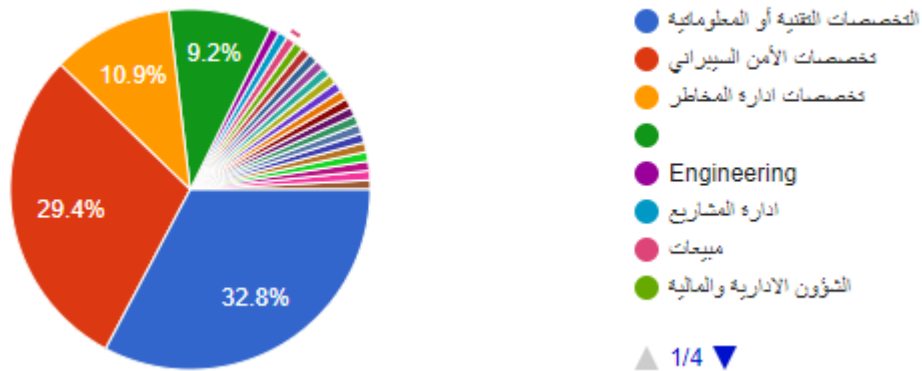
الشكل رقم (٤) توزيع عينة الدراسة حسب الخبرة العملية

٥- حسب مجال العمل / التخصص

جدول (٥-٤) توزيع عينة الدراسة حسب مجال العمل / التخصص

النسبة	التكرار	مجال العمل / التخصص
٢٩.٤%	٣٥	تخصصات الأمن السيبراني
٣٢.٨%	٣٩	التخصصات التقنية
١٠.٩%	١٣	ادارة المخاطر
٩.٢%	١١	تخصص هندسي
٥%	٦	إدارة الأبحاث
١٢.٧%	١٦	الشؤون الادارية والمالية
١٠٠%	١٢٠	المجموع

يتضح من الجدول السابق أن أعلى نسبة في توزيع عينة الدراسة حسب مجال العمل هي: التخصصات التقنية بنسبة ٣٢.٨%، ثم تخصصات الأمن السيبراني بنسبة ٢٩.٤%، ثم الشؤون الادارية والمالية بنسبة ١٢.٧%، ثم ادارة المخاطر بنسبة ١٠.٩%، ثم تخصص هندسي بنسبة ٩.٢%، ثم إدارة الأبحاث بنسبة ٥%. ويتضح ذلك من الشكل التالي:



الشكل رقم (٥) توزيع عينة الدراسة حسب مجال العمل

وللإجابة على أسئلة الدراسة تم حساب المتوسطات الحسابية والانحرافات المعيارية للتعرف على إدارة مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية – بالتطبيق على وزارة الاتصالات وتقنية المعلومات، وكانت النتائج كالتالي:

جدول (٦-٤) المتوسطات الحسابية والانحرافات المعيارية لأبعاد إدارة مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية – بالتطبيق على وزارة الاتصالات وتقنية المعلومات.

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
	إدارة مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية – بالتطبيق على وزارة الاتصالات وتقنية المعلومات.	3.66	66%	0.793		مرتفعة

يتبين من الجدول السابق أن محاور إدارة مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية – بالتطبيق على وزارة الاتصالات وتقنية المعلومات. 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.

٣-٤: 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 ١).

محاور الدراسة:

المحور الأول : اسباب مخاطر الأمن السيبراني في المملكة العربية السعودية

قام الباحث بتخصيص (10) عبارات لتحديد اسباب مخاطر الأمن السيبراني في المملكة العربية السعودية ، وكانت النتائج كالتالي:

جدول (٧-٤) المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات اسباب مخاطر الأمن السيبراني في المملكة العربية السعودية مرتبة تنازليا حسب المتوسطات الحسابية.

م	العبرة	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

م	العبارة	المتوسط الحسابي	النسبة المئوية	الانحراف المعياري	الدرجة	الترتيب
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) وبنسبة 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) وبنسبة مئوية بلغت (60٪).

ويفسر الباحث 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 (٢٠١٧) 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 (٢٠١٧) 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 جزء من سياسات حقوق الطبع لفائدتها على الرغم من كلفتها العالية. كما تتفق تلك النتائج مع دراسة والدو Waldo (٢٠١٨) 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

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

جدول (٤-٨) المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات أهمية الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني مرتبة تنازليا 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	3.36	٪59	0.906	متوسطة	9

م	العبرة	المتوسط الحسابي	النسبة المئوية	الانحراف المعياري	الدرجة	الترتيب
	العلاقة					
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%).

ويفسر الباحث 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 (٢٠١٨) 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 (٢٠١٨) التي أوضحت نتائجها أن اختراق أنظمة المعلومات و نظم الشبكات و المواقع المعلوماتية أصبح خطراً يقلق العديد من المنظمات ، إن هناك

ارتفاعا واضحا في معدل الإختراقات مع تنوع الوسائل المستخدمة في الاختراق على الرغم من سبل الحماية التي تتبعها المنظمات. كما تتفق تلك النتائج مع دراسة فايز (٢٠١٩) التي أوضحت نتائجها أن تكنولوجيا المعلومات تعمل على تطوير أداء الموارد البشرية بالشركة، و أبدى أغلبية عينة الدراسة (٩٨% منهم) شعورهم الإيجابي بأهمية التدريب .

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

قام الباحث بتخصيص (10) عبارات لتحديد طرق تطوير ادارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني. وكانت النتائج كالتالي:

جدول (٩-٤) المتوسطات الحسابية والانحرافات المعيارية والترتيب لعبارات طرق تطوير ادارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني مرتبة تنازليا حسب المتوسطات الحسابية.

م	العبرة	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	3.69	٪67	0.869	مرتفعة	6

م	العبارة	المتوسط الحسابي	النسبة المئوية	الانحراف المعياري	الدرجة	الترتيب
	إلى توسيع التعاون مع المنظمات الدولية الأمنية					
3	تعيين ذوي الخبرة لأعمال تحديد وتقييم المخاطر السيبرانية وتحليل الثغرات الأمنية في الأنظمة والشبكات والإشراف على تحقيق الامتثال 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 وإغلاق 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 إدارة 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) ونسبة 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) ونسبة مئوية بلغت (63٪).

ويفسر الباحث 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 .

وتتفق تلك النتائج مع دراسة إبداع (٢٠١٩) 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 (٢٠٢٠) 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 (٢٠٢١) 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 ليرنر Lerner (٢٠٢١) 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

١-٥ : خلاصة الدراسة

تناولت الدراسة (٥) فصول اشتمل الفصل الأول على مقدمة البحث، وفيه تناول الباحث، ما يلي : مقدمة البحث، المفاهيم الرئيسية في البحث، مشكلة البحث، نموذج ومتغيرات البحث، فروض البحث، أهداف البحث، أهمية البحث، حدود البحث، و هيكل البحث. وتحددت أسئلة الدراسة، فيما يلي :

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

١. التعرف على مخاطر الأمن السيبراني في المملكة العربية السعودية
٢. التعرف على مدى الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية.
٣. 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 تناول الباحث، 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 تناول الباحث تساؤلات الدراسة، وتناول الباحث في الفصل الخامس : خلاصة لأهم نتائج الدراسة وتوصياتها، واشتمل الفصل على ما يلي : خلاصة الدراسة، نتائج الدراسة، توصيات الدراسة، ومقترحات الدراسة.

٢-٥: نتائج الدراسة

- 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).
- 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.
- 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 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 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).
- إن 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).

٣-٥: توصيات الدراسة

يوصي الباحث بضرورة الاهتمام بالتوصيات التالية:

- ينبغي على المؤسسات تحديد المسؤولية المشتركة بين الإدارة التنفيذية و فرق أمن المعلومات وجميع أعضاء المؤسسة فيما يتعلق بإدارة مخاطر الأمن السيبراني. كما يجب أن يعين مسؤول مختص بأمن المعلومات وتوفير الدعم اللازم له لتنفيذ وتنفيذ استراتيجيات الأمن السيبراني.
- يجب على المؤسسات وضع سياسات وإجراءات واضحة للأمن السيبراني تتماشى مع تشريعات الهيئة الوطنية للأمن السيبراني في السعودية. وينبغي أن تشمل هذه السياسات والإجراءات مجموعة من السيطرات والممارسات الأمنية لحماية الأصول الرقمية ومعلومات العملاء والبيانات الحساسة الأخرى.
- يتعين على المؤسسات تنفيذ التدابير الأمنية اللازمة لحماية الأنظمة والشبكات والبيانات الحيوية. ويجب أن تشمل هذه التدابير مجموعة من السيطرات الفنية والتقنيات الأمنية مثل جدران الحماية، وأنظمة الكشف عن التسلل، وتشفير البيانات، وإدارة الهوية والوصول.
- يجب أن تكون المؤسسات ملتزمة بتعزيز التوعية وتوفير التدريب المستمر للموظفين بشأن مخاطر الأمن السيبراني وأفضل الممارسات للوقاية منها.
- ينبغي تعزيز الوعي بحماية المعلومات الحساسة وتحذير الموظفين من التهديدات السيبرانية المحتملة مثل الهجمات الاجتماعية والبريد الإلكتروني الاحتيالي.
- يجب على المؤسسات إجراء تقييم دوري للأمن السيبراني وتحليل الثغرات وتقييم العمليات الأمنية المعمول بها. وينبغي تحديث السياسات والإجراءات وتحسينها بناء على الاستجابة للتهديد .
- ضرورة أن تقوم المؤسسات بوضع استراتيجية شاملة للأمن السيبراني تتضمن تحليل المخاطر وتحديد الأهداف والسياسات المناسبة. ويجب أن تكون هذه الاستراتيجية متوافقة مع تطلعات الشركة ومتطلبات الأعمال والمعايير القانونية والتشريعات الحكومية.

- ينبغي على المؤسسات تخصيص الموارد المالية والبشرية اللازمة لتنفيذ استراتيجية الأمن السيبراني. ويجب تعيين فريق متخصص في أمن المعلومات وتوفير التدريب المناسب لهم للتعامل مع التهديدات السيبرانية المتطورة.
- أن تقوم المؤسسات بتنفيذ تقييم دوري للمخاطر السيبرانية لتحديد الثغرات والضعف في أنظمتها وتحليل الأثر المحتمل للتهديدات. ويساعد ذلك في تحديد أولويات الحماية وتوجيه جهود الأمن السيبراني.
- أن تقوم المؤسسات بتنفيذ مجموعة من التدابير الأمنية لحماية أنظمتها والبيانات الحساسة. ويشمل ذلك تنفيذ التحديثات الأمنية وتطبيق السياسات والإجراءات الأمنية المناسبة مثل وضع كلمات المرور القوية واستخدام تقنيات التشفير وتنفيذ نظام حماية الحواجز النارية.
- أن تقوم المؤسسات بتعزيز التوعية بمخاطر الأمن السيبراني بين الموظفين وتوفير التدريب المستمر لهم. ويشمل ذلك توعية الموظفين بالهجمات السيبرانية المعروفة وتعليمهم أفضل الممارسات للحماية الشخصية والحماية من انتهاكات البيانات والاحتيال الإلكتروني.
- يجب أن تكون المؤسسات قائمة بمراجعة وتقييم سياسات الأمن السيبراني وإجراءاتها بشكل دوري. وأن يتم تحليل الحوادث والانتهاكات السابقة واستخلاص الدروس المستفادة لتحسين أنظمة الأمان وتعزيز القدرة على التعامل مع التهديدات المستقبلية.

٤-٥: مقترحات الدراسة

في ضوء النتائج التي تم التوصل إليها يقدم الباحث بعض التوصيات لدراسات مستقبلية وذلك على النحو التالي:

١. تقييم فاعلية تشريعات الهيئة الوطنية للأمن السيبراني في تحقيق أمان المعلومات في الشركات السعودية التقنية.
٢. تحليل التهديدات السيبرانية الناشئة وتأثيرها على استراتيجيات إدارة المخاطر في الشركات السعودية التقنية.

٣. تقنيات التحقق الثنائي كأداة لتعزيز الأمن السيبراني في الشركات السعودية التقنية:
دراسة مقارنة للممارسات العالمية.
٤. تأهيل الكوادر البشرية لإدارة مخاطر الأمن السيبراني في الشركات السعودية التقنية:
تحليل الاحتياجات وتوجهات المستقبل.
٥. تقييم تأثير الهجمات السيبرانية على أداء الشركات السعودية التقنية واستراتيجيات
الاستجابة المتبعة وفقا لتشريعات الهيئة الوطنية للأمن السيبراني.

قائمة المراجع

المراجع العربية :

- الاتحاد الدولي للاتصالات. (٢٠١٩). الأمن السيبراني في المملكة العربية السعودية. بيروت: مطابع الاتحاد الدولي للاتصالات.
- إبداح، باسم محمد. (٢٠١٩). 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. (٢٠٢١). أمن المعلومات والأمن السيبراني. جدة: جامعة الملك عبد العزيز.
- حمدان، أحمد عبد الله. (٢٠٢١). 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. (٢٠١٦). اتجاهات في أمن المعلومات وأمانها: أهمية تقنيات التعمية - التشفير. المنامة: أكاديمية الخليج العربي للدراسات.
- درويش، محمود أحمد. (٢٠١٨). مناهج البحث في العلوم الإنسانية. الرياض: مكتبة ابن تيمية للنشر.
- الزهراني، أحمد سعيد. (٢٠١٨) آثار قرصنة البرمجيات عالميا. رسالة ماجستير منشورة. كلية العلوم الإستراتيجية. جامعة نايف العربية للعلوم الأمنية: الرياض
- السالمي، علاء الكيلاني. (٢٠١٩). أساسيات نظم المعلومات الإدارية. مكتبة وائل: عمان.
- سكيكر، محمد علي. (٢٠٢٢). الجريمة المعلوماتية و كيفية التصدي لها. ط٢. الدار البيضاء: دار النشر المغربية.
- السهلي، فارس بن صالح. (٢٠١٩). نطاق مسؤولية الناقل الجوي للركاب وأساسها في نظام الطيران المدني السعودي. الرياض: مطابع وزارة الداخلية.
- الشراري، خالد جويش. (٢٠١٧): الأمن السيبراني في المملكة العربية السعودية. الرياض: مكتبة دار القلم.

- الصيدلاني، خالد صالح.(٢٠١٧). واقع قرصنة البرمجيات في الأردن وسبل مواجهتها. رسالة ماجستير منشورة. كلية الأعمال : الجامعة الأردنية.
- عبد ربه ، رائد محمد. (٢٠٢٠). مبادئ نظم المعلومات الإدارية. بيروت: مكتبة بيروت الحرة.
- عطوان، أسعد محمد. (٢٠١٦). مناهج البحث العلمي. ط٢. القاهرة: مكتبة دار المعارف.
- العضياني ، ماجد محمد . (٢٠١٨). انتهاك خصوصية البيانات في مؤسسات الأعمال وأثره على أداء المؤسسات . رسالة ماجستير منشورة .كلية التجارة . القاهرة : جامعة القاهرة .
- الغامدي، محمد حسن. (٢٠٢١). فرص حلول الأمن السيبراني في المملكة العربية السعودية . الرياض: مطابع فنتك السعودية.
- فايز ، وائل علي. (٢٠١٩). دور تكنولوجيا المعلومات في تدعيم أداء الموارد البشرية (دراسة ميدانية). رسالة ماجستير منشورة . كلية التربية. المنصورة: جامعة المنصورة.
- القحطاني ، منصور سعيد. (٢٠١٩). مهددات الأمن المعلوماتي وسبل مواجهتها. ط٢. الرياض : مكتبة دار القلم .
- الكبيسي، حامد جهاد. (٢٠١٩). 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 . (٢٠٢١). أثر كفاءة أداء الموارد البشرية على سلامة الطيران المدني بالتطبيق على قطاع الطيران المدني المصري. القاهرة : أكاديمية السادات.
- الهيئة الوطنية للأمن السيبراني. (٢٠١٨). التعريف بالهيئة الوطنية للأمن السيبراني . الرياض : مطابع وزارة الداخلية.
- الهيئة الوطنية للأمن السيبراني. (٢٠١٨). الضوابط الأساسية للأمن السيبراني في المملكة العربية السعودية . الرياض: مطابع وزارة الإعلام.
- الهيئة العامة للإحصاء. (٢٠١٨). موجز إحصاءات هيئة الطيران المدني بالمملكة العربية السعودية. الرياض: مطابع الهيئة العامة للإحصاء.
- ياغي، محمد. (٢٠١٧). 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 (١) استبانة التطبيق

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

والصلاة والسلام على أشرف الخلق والمرسلين نبينا محمد الصادق الأمين وعلى آله وصحبه
أجمعين

إلى السادة منسوبي :وزارة الاتصالات وتقنية المعلومات.

السلام عليكم ورحمة الله وبركاته أما بعد،،

أتقدم بالشكر الجزيل سلفاً على تكرمكم بالإجابة على هذه الاستبانة، والتي تهدف إلى جمع
البيانات لتخدم بحث التخرج لدرجة الماجستير تحت عنوان:(إدارة مخاطر الأمن السيبراني
في المؤسسات الحكومية بالمملكة العربية السعودية – بالتطبيق على وزارة الاتصالات
وتقنية المعلومات).

كما أمل تفضلاً بأن تكون الاجابات دقيقة وموضوعية لمحاو 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

الباحث

الجزء الأول (البيانات الأولية):

١- العمر من:

- ☐ ٣٠ سنة فأقل
- ☐ ٣١ إلى ٤٠ سنة
- ☐ ٤١ إلى ٥٠ سنة
- ☐ ٥١ فأكثر

٢- المؤهل العلمي:

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

٣- المستوى الوظيفي:

- ☐ مدير
- ☐ مشرف
- ☐ موظف

٤- الخبرة العملية:

- ☐ ٥ سنوات فأقل
- ☐ من ٦ إلى ١٠ سنوات
- ☐ أكثر من ١١ سنة

٥- مجال العمل أو التخصص:

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

الجزء الثاني (محاوَر الاستبانة (١/٣):

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
١	هجمات القرصنة الإلكترونية ومحاولات اختراق الأنظمة السيبرانية والحصول على معلومات حساسة أو التلاعب بها				
٢	سرقة المعلومات الحساسة والتجسس على الأنشطة الحكومية والخاصة				
٣	التصيد الإلكتروني عبر الإنترنت مثل الرسائل الاحتيالية، وسرقة الحسابات البنكية				
٤	الهجمات التي تستهدف إعاقة البنية التحتية السيبرانية للمملكة، مثل تعطيل خدمات الإنترنت				
٥	الاختراقات السيبرانية أو الأمنية للمؤسسات الحكومية والشركات والتي تهدد سرية المعلومات والملكية الفكرية وسلامة الأنظمة				
٦	تهديدات البرمجيات الخبيثة والفايروسات التي يتم استخدامها لاختراق الأنظمة وتدمير البيانات أو سرقتها				
٧	انتهاكات الخصوصية وتسريب المعلومات الشخصية للأفراد				
٨	الهجمات السيبرانية على البنية التحتية الحيوية مثل الشبكات الكهربائية والماء والنقل				
٩	الاحتيال المصرفي وسرقة المعلومات المالية مما يتسبب في خسائر مالية كبيرة				
١٠	تهديدات الهجمات السيبرانية على البنية الحيوية الوطنية مثل القطاعات النفطية والنقل والصناعة				

الجزء الثاني (محاورة الاستبانة (٢/٣):

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
١	تعيين فريق متخصص في الأمن السيبراني				
٢	اعداد تقارير دورية عن تقييمات الأمن السيبراني وتحديد نقاط الضعف وخطط المعالجة				
٣	انشاء برنامج خاص بالتوعية بالأمن السيبراني، بالإضافة إلى الاستثمار في تدريب الموظفين حول قضايا الأمن السيبراني				
٤	تحديد واعتماد وثيقة لسياسات واجراءات الأمن السيبراني ويتم تطبيقها بشكل منتظم				
٥	العمل على اعداد وتقديم تقارير مفصلة عن الاستجابة للحوادث السيبرانية وتحليلها ومشاركتها مع أصحاب العلاقة				
٦	العمل على المراجعات الدورية لتحقيق من الامتثال لتشريعات الهيئة الوطنية للأمن السيبراني				
٧	التعاون مع القطاعات الخاصة والحكومية في المملكة لتبادل المعلومات والمنفعة لتعزيز الأمن السيبراني				
٨	الاستثمار لتطوير تقنيات تعزيز الأمن السيبراني				
٩	التعاون بشكل وثيق مع الهيئة الوطنية للأمن السيبراني في تنفيذ الضوابط والتشريعات الأمنية اللازمة				
١٠	توثيق واعتماد استراتيجية للأمن السيبراني تتضمن الأهداف والمبادرات والمشاريع الخاصة في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة				

الجزء الثاني (محاور الاستبانة (٣/٣):

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

ملحق (٢)
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.

Verify Report:
Scan this QR Code



Midocean University

College of Management

Department of business management

**Cybersecurity Risk Management in Government Institutions in the Kingdom
of Saudi Arabia – Applied to the Ministry of Communications and Information
Technology**

Prepared by:

Supervised by:

Year:2024