

جامعة ميدأوشن

كلية الإدارة

قسم / تخصص ادارة المخاطر



سُبل ادارة مخاطر الأمن السيبراني في الشركات السعودية الخاصة بحسب تشريعات الهيئة الوطنية للأمن
السيبراني

دراسة عينة تطبيقية لبعض من المؤسسات التكنولوجية بمنطقة الرياض

إعداد الطالبة /

هُتاف بنت عبدالله خليل

إشراف /

د. وليد عبدالجواد سليمان صديق

د. الفيصّل عبدالحميد محمد حسن

العام الدراسي:

2023

خطة البحث:

- المقدمة.
- مشكلة الدراسة.
- أهمية الدراسة.
- أهداف الدراسة.
- تساؤلات الدراسة (الفروض).
- الدراسات السابقة.
- المنطلقات النظرية للدراسة
- المنهجية وطرق البحث.
- أدوات الدراسة (أدوات جمع البيانات).
- مجالات الدراسة (بشري، مكاني، زمني).
- المراجع والمصادر

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 عالمياً؛ ومراجعة سياساتها واجرائتها بشكل دوري للتأكد من الامتثال لهذه المعايير واشعار الهيئة بالانتهاكات الأمنية واخذ الاجراء المناسب.

تتناول الباحثة في هذه الدراسة موضوع سبل ادارة 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 نهجاً 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 سبل ادارة 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 ادارة 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 ادارة مخاطر السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني.

- تساؤلات الدراسة (الفروض).

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

1. ما هي مخاطر ادارة الأمن السيبراني في المملكة العربية السعودية؟
2. ما مدى الإلتزام بتشريعات الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية؟
3. ما سبب تفعيل ادارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني؟

- الدراسات السابقة.

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 جبهة 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 إبداح (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 نموذجا عن شركات التأمين في العراق وباختبار عينة من المديرين والموظفين العاملين في الشركتين وبعده (70) موظفا، 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 (أنتويرب) 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 الدراسات 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 الإحصائية المناسبة
- تحليل وتفسير النتائج التي توصلت إليها الدراسة

ثانيًا: الاطار النظري تتناول الباحثة في الاطار النظري مايلي:

- مفهوم الأمن السيبراني
- أهمية الأمن السيبراني
- أهداف الأمن السيبراني
- العناصر الأساسية للأمن السيبراني
- عوامل تحقيق الأمن السيبراني
- مخاطر الأمن السيبراني
- استراتيجيات ادارة مخاطر الأمن السيبراني
- الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية
- تشريعات الهيئة الوطنية للأمن السيبراني
- سبل تعزيز الأمن السيبراني في المملكة العربية السعودية

تتمثل النظريات المفسرة لإدارة مخاطر الأمن السيبراني، فيما يلي:

- 1- نظرية النموذج الدائري للأمن السيبراني (Cybersecurity Diamond Model): تعتبر هذه النظرية منهجًا 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 إطارًا لتحليل المخاطر وتصميم استراتيجيات الحماية.
- 2- نظرية الانحدار العُقدِي 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 جزءًا أساسيًا من هذه النظرية.
- 5- نظرية النموذج العام للتهديدات السيبرانية (General Model of Cyber Threats): تقدم هذه النظرية نموذجًا 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 تأثيرًا.

7- نظرية الاستجابة للحوادث السيبرانية (Incident Response Theory): تهدف هذه النظرية إلى تطوير إطار عمل للاستجابة الفعالة للحوادث السيبرانية. وتشمل هذه النظرية اجراءات 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 الدراسة (أدوات جمع البيانات).

أداة البحث:

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
 - المحور الثاني: مدى الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني
 - المحور الثالث: سبل تفعيل إدارة 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 الرياض

• الحدود الزمنية:

سوف تجري الدراسة خلال العام 1445هـ / 2023م.

المراجع والمصادر:

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.
- الشراري، 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 .
- الكيسي، 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.

Midocean University



College of Management

Department of Risk Management

**Ways to Cybersecurity Risk Management in Private Saudi Companies according to the
Legislation of the National Cybersecurity Authority**

An applied case study of some of Information Technology Companies in Riyadh

Prepared by:

Hotaf Abdullah Khalil

Supervised by:

Dr. Walid Abdul Jawad Suliman Siddeq

Dr. Al-Faisal Abdulhamid Mohammed Hasan

Year:2023