



عنوان البحث:

**دور إدارة المخاطر واستمرارية أعمالها في مراكز البيانات للحد من الهجمات
السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة
العربية السعودية**

مشروع بحث استكمالاً لمتطلبات الحصول على درجة الماجستير

إعداد الطالب:

مشاري بن عبد الحسن بن محمد بن سلوم

الرقم الجامعي: 241001832

إشراف الدكتور:

أسماء أبو عنزه

الخام الدراسي

٢٠٢٤م





فهرس المحتويات



م	الموضوع	الصفحة
١.	آية قرآنية.....	٢
٢.	فهرس المحتويات	٣
٣.	قائمة الجداول	٧
٤.	قائمة الأشكال	٨
٥.	ملخص الدراسة	٩
٦.	الفصل الأول : الإطار العام للدراسة	١١
٧.	مقدمة الدراسة	١٢
٨.	مشكلة الدراسة	١٣
٩.	أهمية الدراسة.....	١٦
١٠.	أهداف الدراسة	١٨
١١.	أسئلة الدراسة.....	٢١
١٢.	فروض الدراسة	٢٢
١٣.	الدراسات السابقة	٢٤
١٤.	التعليق على الدراسات السابقة	٢٥
١٥.	المنطلقات النظرية للدراسة	٢٧
١٦.	منهجية الدراسة	٢٨
١٧.	أدوات الدراسة	٢٩
١٨.	حدود الدراسة	٣١



٣٣	الفصل الثاني: الإطار النظري	١٩
٣٣	المبحث الأول: إدارة المخاطر	٢٠
٣٤	التعريف بمفهوم الخطر	٢١
٣٤	التعريف بإدارة المخاطر	٢٢
٣٥	أهمية إدارة المخاطر	٢٣
٣٦	مراحل عملية إدارة المخاطر	٢٤
٣٨	المبحث الثاني: الأمن السيبراني	٢٥
٣٩	مفهوم الأمن السيبراني	٢٦
٤٠	مجالات الأمن السيبراني	٢٧
٤١	أهداف الأمن السيبراني	٢٨
٤٣	مخاطر الهجمات السيبرانية	٢٩
٤٥	ادارة مخاطر الأمن السيبراني	٣٠
٤٦	دور إدارة المخاطر في الأمن السيبراني والحد من الجريمة الإلكترونية	٣١
٤٨	طرق تعزيز الأمن السيبراني	٣٢
٥٠	الفصل الثالث: منهجية وإجراءات الدراسة	٣٣
٥١	منهج الدراسة	٣٤
٥٢	مجتمع الدراسة	٣٥
٥٢	عينة الدراسة	٣٦



٥٣	أداة الدراسة.....	٣٧.
٥٤	صدق الأداة.....	٣٨.
٥٧	ثبات الأداة.....	٣٩.
٦٠	إجراءات الدراسة.....	٤٠.
٦٠	متغيرات الدراسة.....	٤١.
٦٢	الفصل الرابع: منهجية وإجراءات الدراسة.....	٤٢.
٦٢	تحليل وعرض النتائج ومناقشتها	٤٣.
٦٣	تحليل البيانات الديموغرافية لعينة الدراسة	٤٤.
٦٧	تحليل محتويات الإستبانة	٤٥.
٨١	النتائج	٤٦.
٨٣	التوصيات	٤٧.
٨٦	قائمة والمراجع	٤٨.
٩٢	الملاحق	٤٩.

قائمة الجداول:

- جدول ١ معامل ارتباط بيرسون لمحاور الاستبيان 65
- جدول ٢ قيم معاملات ألفا كرونباخ لأداة الدراسة. 57
- جدول ٣ خصائص عينة الدراسة وفقاً لمتغير النوع. 63
- جدول ٤ توزيع خصائص عينة الدراسة وفقاً لمتغير عدد سنوات الخبرة 64
- جدول ٥ المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة
عن المحور الأول. 67
- جدول ٦ المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة
عن المحور الثاني. 68
- جدول ٧ المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة
عن المحور الثالث. 69
- جدول ٨ نتائج تحليل الإنحدار الخطي البسيط للفرضية الأولى. 70
- جدول ٩ نتائج تحليل الإنحدار الخطي البسيط للفرضية الأولى. 72
- جدول ١٠ نتائج تحليل الإنحدار الخطي البسيط للفرضية الثالثة. 75
- جدول ١١ إختبار لقياس دلالة الفروق لمحاور الإستبيان وفقاً لمتغير النوع. 77
- جدول ١٢ تحليل التباين الأحادي One Way ANOVA لمحاور الإستبيان
وفقاً لمتغير عدد سنوات الخبرة. 78
- جدول ١٣ إختبار لقياس دلالة الفروق لمحاور الإستبيان وفقاً لمتغير المؤهل العلمي. 79

قائمة الأشكال:

- شكل ١ توضيح خصائص عينة الدراسة وفقاً لمتغير الجنس. 63
- شكل ٢ توزيع خصائص عينة الدراسة وفقاً لمتغير عدد سنوات الخبرة 65
- شكل ٣ توزيع خصائص عينة الدراسة وفقاً لمتغير المؤهل العلمي. 66
- شكل ٤ الإنحدار الخطي للفرضية الأولى. 72
- شكل ٥ الإنحدار الخطي البسيط للفرضية الثانية. 74
- شكل ٦ الإنحدار الخطي البسيط للفرضية الفرعية الثالثة. 76



ملخص الدراسة:

هدفت هذه الدراسة إلى إستكشاف دور إدارة المخاطر وإستمرارية الأعمال في تعزيز أمن وحماية مراكز البيانات في القطاعين الحكومي والأهلي، ومعرفة الممارسات والتقنيات المتبعة في هذا المجال، والتحديات التي تواجه تطبيقها، بالإضافة إلى التوصيات والسبل الكفيلة بتعزيز قدرة هذه المراكز على مواجهة التهديدات السيبرانية والحفاظ على سرية ونزاهة البيانات الحساسة.

وإستمرارية الأعمال التقنية هي مجموعة من الخطط والإجراءات التي تضمن إستمرارية تشغيل الأنظمة التقنية والبيانات والبرامج الحيوية للمنظومة في حالات الطوارئ أو الإنقطاعات المفاجئة، تشمل هذه الطوارئ الكوارث الطبيعية، الهجمات السيبرانية، الأعطال التقنية الى معرفة دور إدارة المخاطر، وإستمرار الأعمال التقنية، التي تعتبر مجموعة من الخطط والإجراءات التي تضمن إستمرارية تشغيل الأنظمة التقنية والبيانات والبرامج الحيوية للمنظومة في حالات الطوارئ أو الانقطاعات المفاجئة، تشمل هذه الطوارئ الكوارث الطبيعية، الهجمات السيبرانية، الأعطال التقنية، تشمل ذلك تقييم المخاطر، وتطوير إستراتيجيات للتعامل معها، وضمان توافر البيانات بشكل آمن وسري، إستمرارية الأعمال التقنية تعني الحفاظ على توافر وإستمرارية الأنظمة والتقنيات الحاسوبية الحيوية للمنظومة.



شكلت هذه الدراسة أهمية بالغة تمثلت في تحديد المخاطر والعمل على معرفة الهجمات السيبرانية على مراكز البيانات، وما هي الأمور الواجب إتباعها لإستمرارية عمل مراكز البيانات.

إستخدم الباحث في البحث المنهج الوصفي التحليلي، والمنهج الإستقرائي، والمنهج الوثائقي، والمنهج المسحي، للوصول الى النتائج المطلوبة، وقد توصلت الدراسة الى أنه يوجد أثر ذو دلالة إحصائية لتقييم إجراءات إدارة المخاطر السيبرانية في المراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية، لا توجد فروض ذات دلالة إحصائية لدور إدارة المخاطر وإستمرارية أعمالها في المراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية تعزي لمتغير النوع والخبرة والمؤهل العلمي، وأوصت الدراسة بتطوير استراتيجيات شاملة لإدارة المخاطر السيبرانية للتركز على تحليل التهديدات، وتقييم احتمالات الإختراق، ووضع خطط استجابة فورية، ويجب تطبيق برامج تدريبية دورية للموظفين لتعزيز الوعي السيبراني، مع تزويدهم بالأدوات اللازمة للتعامل مع الهجمات الإلكترونية وتجنب الأخطاء البشرية التي تؤدي إلى الإختراقات



الفصل الأول

إطار الدراسة العام .

- ◆ مقدمة الدراسة .
- ◆ مشكلة الدراسة .
- ◆ أهمية الدراسة .
- ◆ أهداف الدراسة ..
- ◆ أسئلة الدراسة .
- ◆ فروض الدراسة .
- ◆ الدراسات السابقة .
- ◆ المنطلقات النظرية للدراسة .
- ◆ منهج الدراسة ..
- ◆ حدود الدراسة ..
- ◆ مراجع الدراسة ..



◆ مقدمة الدراسة:

الحمد لله أهل الحمد ومستحقه، حمداً يفضل على كل حمد، كفضل الله على خلقه، وأشهد أن لا إله إلا الله وحده لا شريك له شهادة قائم بحقه، وأشهد أن محمداً عبده ورسوله غير مرتاب في صدقه، صلى الله عليه وسلم وصحبه وسلم ما جاد سحاب بودقه، وما رعد برقه أما بعد:

إستمارية الأعمال التقنية هي مجموعة من الخطط والإجراءات التي تضمن إستمرارية تشغيل الأنظمة التقنية والبيانات والبرامج الحيوية للمنظومة في حالات الطوارئ أو الانقطاعات المفاجئة، تشمل هذه الطوارئ الكوارث الطبيعية، الهجمات السيبرانية، الأعطال التقنية، أو أي حدث غير متوقع يمكن أن يؤثر على العمليات اليومية يجب تفعيل دور إدارة المخاطر في مراكز البيانات لضمان إستمرارية أعمالها وحماية بياناتها من الهجمات السيبرانية التي تشكل خطراً على البيانات الحساسة، تشمل ذلك تقييم المخاطر، وتطوير إستراتيجيات للتعامل معها، وضمان توافر البيانات بشكل آمن وسري، استمرارية الأعمال التقنية تعني الحفاظ على توافر وإستمارية الأنظمة والتقنيات الحاسوبية الحيوية للمنظومة، حيث تشمل هذه الجوانب تخطيط وتنفيذ إستراتيجيات وإجراءات لضمان إستمرارية الأنظمة والبيانات والبرامج التقنية الأساسية للمنظومة في حالات الطوارئ أو الكوارث الطبيعية.



في ظل التقدم التكنولوجي المتسارع وإزدیاد إعتیاد المؤسسات الحكومية والخاصة على تقنية المعلومات، أصبحت مراكز البيانات محور أساسي لعمليات الأعمال والخدمات الحيوية ومع ذلك، فإن هذه المراكز تواجه تهديدات متزايدة من الهجمات السيبرانية وفقد البيانات الحساسة، مما يشكل خطراً كبيراً على إستمرارية الأعمال والسمعة المؤسسية.

في هذا السياق، تبرز أهمية إدارة المخاطر واستمرارية الأعمال كأدوات فعالة للتصدي لهذه التحديات في مراكز البيانات، إدارة المخاطر تسمح بتحديد وتقييم المخاطر المحتملة وتطوير خطط للتخفيف منها، بينما تضمن إستمرارية الأعمال قدرة المؤسسة على الإستجابة والتعافي من أي حوادث أو كوارث تؤثر على عملياتها.

◆ مشكلة الدراسة:

مراكز البيانات هي مرافق تخزين تستضيف أنظمة الحوسبة والشبكات التي تدعم أنشطة الأعمال الرقمية، إدارة المخاطر في مراكز البيانات وكيفية تحليلها والتخطيط للتعامل معها بشكل آمن و يشمل ذلك تحديد المخاطر، وتقييمها . لتأثير المخاطر على استمرارية العمل وسلامة البيانات، فقدان البيانات أو توقف الخدمة يمكن أن يؤدي إلى خسائر مالية كبيرة وتأثير سلبي على سمعة المنظومة.



تواجه المنظومات الحكومية والأهلية تحديات كبيرة في حماية مراكز البيانات الخاصة بها من الهجمات السيبرانية المتزايدة والمعقدة. تكمن مشكلة الدراسة في تحديد الفجوات الأمنية الحالية في هذه المنظومات، وتقييم مدى فعالية الإجراءات والتقنيات المستخدمة في إدارة وحماية مراكز البيانات من التهديدات السيبرانية، كما تسعى الدراسة إلى فهم العوامل التي تؤثر على قدرة هذه المنظومات في التصدي للهجمات، وتقديم حلول مبتكرة لتعزيز مستوى الأمان وضمان إستمرارية الأعمال.

١- تحديد وتقييم المخاطر: يعتبر تحديد وتقييم المخاطر المحتملة التي يمكن أن تؤثر على مراكز البيانات مهمة صعبة بسبب التغيرات المستمرة في التهديدات السيبرانية والتقنيات المستخدمة، البحث في كيفية تطوير نماذج تقييم مخاطر فعالة ومحدثة يُعد محوري.

٢- تصميم إستراتيجيات استمرارية الأعمال: تطوير خطط إستمرارية الأعمال التي تضمن إستعادة البيانات وإستمرارية الخدمات بعد حدوث هجمة سيبرانية أو أي نوع من الانقطاعات، تحديد أفضل الممارسات والحلول التقنية لضمان الإستجابة السريعة والفعالة هو تحدٍ بحثي.

٣- التكامل بين الأمان السيبراني وإستمرارية الأعمال: غالباً ما تُدار المخاطر وإستمرارية الأعمال كعمليتين منفصلتين، البحث في كيفية تكامل هاتين العمليتين بشكل فعال لتحقيق حماية أفضل يمثل تحدياً كبيراً.



٤- الإمتثال للتشريعات والمعايير: مراكز البيانات، خاصة في القطاعات الحكومية والأهلية، يجب أن تلتزم بمجموعة معقدة من القوانين والمعايير، البحث في كيفية تحقيق هذا الامتثال بكفاءة مع الحفاظ على مستويات عالية من الأمان وإستمرارية الأعمال هو مجال حيوي.

٥- تحديات التقنية والبنية التحتية: تطوير وصيانة بنية تحتية قوية لمراكز البيانات يتطلب إستثمارات كبيرة وبحثاً مستمراً في التقنيات الجديدة، البحث في كيفية تحسين هذه البنية لتحمل الهجمات وضمان أعلى مستويات الأداء والأمان هو أيضاً تحدي بحثي.

٦- التدريب والوعي الأمني: غالباً ما يتم إغفال أهمية التدريب ورفع وعي الموظفين بأمان المعلومات، البحث في أفضل الطرق لتدريب الموظفين وتحسين وعيهم بالمخاطر وكيفية التعامل معها يعد جزءاً لا يتجزأ من تعزيز الأمان في مراكز البيانات.

تكمّن العديد من المؤثرات المعلومة والغير معلومة التي بدورها تشكل أخطر الرئيسي في مراكز البيانات ومن أهمها عدم الإلتزام الكامل بالمعايير والأنظمة الخاصة بها والتي من شأنها ان تكون اول أبواب الخطر.

من ضمن المعايير المهمة والغير ملتزم بها في كثير من الجهات هو النطاق الجغرافي لمراكز البيانات حيث أنه من الواجب أن تكون في المدن الصحراوية



تحت الأرض وفي المدن الساحلية يتوجب وضعها أعلى من مستوى سطح البحر.

◆ أهمية الدراسة:

إدارة المخاطر في مراكز البيانات تعد من العوامل الحيوية التي تضمن إستمرارية العمل وحماية البيانات الحيوية. مع تزايد الإعتماد على التقنيات الجديدة والبيانات، أصبحت مراكز البيانات هدفاً رئيسياً للهجمات السيبرانية والكوارث الطبيعية والمشاكل التقنية، لذا، فإن تنفيذ استراتيجيات فعالة لإدارة المخاطر يمكن أن يقلل من تأثير هذه التهديدات ويحافظ على سلامة البيانات وإستمرارية أعمال المنظومة.

الأهمية العملية:

١- تحديد المخاطر: بتحديد المخاطر المحتملة، يمكن أن تشمل هذه المخاطر الهجمات السيبرانية، إنقطاع التيار الكهربائي، الكوارث الطبيعية، والأخطاء البشرية.

٢- التقييم: بعد تحديد المخاطر، يتم تقييم مدى تأثير كل خطر على مركز البيانات يتم ذلك من خلال تحليل الإحتمالية والتأثير المحتمل لكل خطر.



٣- التخطيط: بعد تقييم المخاطر، يتم وضع خطط للتعامل معها، يمكن أن تشمل هذه الخطط إستراتيجيات الوقاية، وخطط الطوارئ، وإجراءات الإستجابة السريعة.

٤- التنفيذ: يتم تنفيذ الخطط الموضوعة للتعامل مع المخاطر، يشمل ذلك تدريب الموظفين، وتحديث الأنظمة، وتطبيق الإجراءات الوقائية.

٥- المراقبة والمراجعة: يتم مراقبة فعالية الخطط والإجراءات المتبعة بانتظام، ومراجعتها وتحديثها حسب الحاجة لضمان إستمرار فعاليتها.

في العصر الرقمي الحالي، أصبحت مراكز البيانات القلب النابض للمنظومات الحكومية والأهلية، حيث تعتمد عليها المؤسسات بشكل كبير في تخزين ومعالجة البيانات الحساسة، ومع تزايد التهديدات السيبرانية، أصبحت إدارة مخاطر هذه المراكز ضرورة ملحة لضمان حماية البيانات وإستمرارية الأعمال، يهدف هذا البحث إلى استكشاف إستراتيجيات وأساليب إدارة مخاطر مراكز البيانات من الهجمات السيبرانية، مع التركيز على المنظومات الحكومية والأهلية، سيتم تسليط الضوء على التحديات التي تواجهها هذه المؤسسات، وأهمية تطوير سياسات أمنية فعالة، وتبني تقنيات حديثة لحماية البنية التحتية الرقمية. من خلال هذا البحث، نسعى إلى تقديم توصيات عملية لتعزيز الأمن السيبراني وضمان سلامة البيانات في مواجهة التهديدات المتزايدة.



الأهمية العلمية:

- ١- تعتبر الأهمية العلمية لهذه الدراسة في أنها تبحث وبشكل تفصيلي عن دور إدارة المخاطر وإستمرارية أعمالها في مراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية، حسب المنهجية العلمية مما يجعل لها أهمية كبيرة.
- ٢- تحتوي هذه الدراسة نتائج معلومات مهمة، تعتبر رافدا علميا، تمكن للباحثين والدارسين الإستفادة منها.

♦ أهداف الدراسة:

يهدف هذا البحث إلى إستكشاف دور إدارة المخاطر وإستمرارية الأعمال في تعزيز أمن وحماية مراكز البيانات في القطاعين الحكومي والأهلي، سوف يتناول البحث الممارسات والتقنيات المتبعة في هذا المجال، والتحديات التي تواجه تطبيقها، بالإضافة إلى التوصيات والسبل الكفيلة بتعزيز قدرة هذه المراكز على مواجهة التهديدات السيبرانية والحفاظ على سرية ونزاهة البيانات الحساسة.

إستمرارية الأعمال التقنية هي مجموعة من الخطط والإجراءات التي تضمن أستمارية تشغيل الأنظمة التقنية والبيانات والبرامج الحيوية للمنظومة في حالات



الطوارئ أو الانقطاعات المفاجئة، تشمل هذه الطوارئ الكوارث الطبيعية، الهجمات السيبرانية، الأعطال التقنية، أو أي حدث غير متوقع يمكن أن يؤثر على العمليات اليومية، تتضمن الأهداف الرئيسية للدراسة ما يلي:

- أهمية إستمرارية الأعمال التقنية:

أ- حماية البيانات: تضمن إستمرارية الأعمال التقنية حماية البيانات الحيوية من الفقدان أو التلف.

ب- تقليل التوقف أعمال المنظومة: تساعد في تقليل فترة التوقف عن العمل، مما يضمن إستمرارية العمليات الحيوية للمنظومة بشكل فعال.

ج- الإمتثال التنظيمي: تساعد المؤسسات في الإمتثال للمتطلبات القانونية والتنظيمية المتعلقة بحماية البيانات وإستمرارية الأعمال.

د- الحفاظ على السمعة: تضمن إستمرارية الأعمال التقنية الحفاظ على سمعة المؤسسة من خلال تقديم خدمات متواصلة وموثوقة.

هـ- الإستجابة السريعة للطوارئ: تتيح للمؤسسات الإستجابة السريعة والفعالة للطوارئ، مما يقلل من تأثير الأحداث السلبية.



- أهداف يلزم تطبيقها:

أ- تحسين فهم المخاطر السيبرانية: تعزيز القدرة على تحديد، تقييم، وفهم المخاطر السيبرانية التي يمكن أن تؤثر على مراكز البيانات، هذا يشمل تطوير نماذج لتحليل المخاطر بشكل دقيق ومستمر

ب- تطوير إستراتيجيات إستمرارية الأعمال: صياغة وتنفيذ خطط إستمرارية الأعمال التي تضمن عدم التوقف الكامل للعمليات في حالة حدوث هجمات سيبرانية أو أي اضطرابات أخرى، الهدف هو تقليل الوقت اللازم لإستعادة الخدمات والمحافظة على الكفاءة التشغيلية.

ج- تكامل الأمان السيبراني مع إستمرارية الأعمال: تعزيز التكامل بين إدارة المخاطر السيبرانية وخطط إستمرارية الأعمال لضمان تنفيذ إستجابة شاملة ومتكاملة عند الضرورة.

د- الإمتثال للمعايير والتنظيمات: ضمان أن مراكز البيانات تلتزم بالمعايير والتشريعات المحلية والدولية المتعلقة بالحماية السيبرانية وخصوصية البيانات، الهدف هو تعزيز الثقة في الأنظمة الحكومية والأهلية من خلال الإمتثال الصارم.

هـ- تحسين البنية التحتية والتقنيات: إستثمار في أحدث التقنيات وتحديث البنية التحتية لتعزيز القدرة على مواجهة التهديدات السيبرانية وتحسين الأداء العام لمراكز البيانات.



و- تعزيز الوعي والتدريب: رفع مستوى الوعي والتدريب للموظفين فيما يخص الممارسات الأمنية وإدارة المخاطر، وذلك لتقليل الأخطاء البشرية وتحسين الإستجابة للحوادث.

ز- تقييم وتحسين الممارسات الحالية: إجراء تقييمات دورية للممارسات والإجراءات الحالية وتحديثها بناء على النتائج لضمان الفعالية المستمرة في حماية البيانات والأنظمة.

◆ أسئلة الدراسة:

يمكن تقسيم أسئلة الدراسة التي بين أيدينا الى ما يلي:

ما هو الأثر المترتب عليه أكثر المخاطر في مراكز البيانات ؟

تحليل الأثر على الأعمال هو عملية تحديد وتقييم تأثير الإنقطاعات المحتملة على العمليات الحيوية للمؤسسة، يساعد هذا التحليل في تحديد الأولويات ووضع استراتيجيات لاستعادة الأنظمة والبيانات بسرعة، يتمثل في تحديد وتقييم المخاطر المحتملة التي قد تؤثر على إستمرارية الأعمال التقنية. يشمل ذلك تحليل التهديدات الداخلية والخارجية وتحديد نقاط الضعف في الأنظمة التقنية، يجب وضع خطة الطوارئ واضحة ومنظمة يتم إتباعها في حالة حدوث إنقطاع، تشمل هذه الخطة تفاصيل حول كيفية إستعادة الأنظمة



والبيانات، وتحديد المسؤوليات، وتوفير الإتصالات اللازمة، يجب على المختصين التقنيين تنفيذ إستراتيجيات فعالة للنسخ الإحتياطي وإستعادة البيانات لضمان حماية البيانات الحساسة ويشمل ذلك النسخ الإحتياطي الدوري للبيانات وتخزين النسخ الإحتياطية في مواقع آمنة خارج المنظومة ولا يتم الوصول إليها إلا بموافقة المسؤولين المختصين التقنيين ومسؤولين إدارة المخاطر، على جميع المنظومات تدريب الموظفين على خطط الطوارئ وإجراءات إستمرارية الأعمال التقنية، يساعد ذلك في ضمان إستجابتهم السريعة والفعالة في حالة حدوث طوارئ.

◆ فروض الدراسة:

تطبيق الدراسة وفروضها على عدد من المنشآت الصغيرة والمتوسطة الحكومية والأهلية ويشمل ذلك التأكد من البنى التحتية وخطط الطوارئ لمراكز البيانات في حال حدوث هجمات سيبرانية أو خطأ بشري، وتتمثل بالاتي:

١- فرضية تطبيق إجراءات أمنية محدثة: تطبيق إجراءات أمنية محدثة ومتطورة في مراكز البيانات يقلل من إحتمالية الهجمات السيبرانية وفقدان البيانات الحساسة في المنظومات الحكومية والأهلية.



٢- فرضية التدريب والوعي: تحسين مستويات التدريب والوعي الأمني لدى الموظفين يقلل من مخاطر الهجمات السيبرانية والأخطاء البشرية التي قد تؤدي إلى فقدان البيانات.

٣- فرضية الاستثمار في التكنولوجيا: الاستثمار في تكنولوجيا متقدمة للحماية من الهجمات السيبرانية يعزز من قدرة المنظومة الحكومية والأهلية على حماية بياناتها الحساسة.

٤- فرضية التعاون بين المؤسسات: التعاون والتنسيق بين المؤسسات الحكومية والأهلية يحسن من كفاءة إدارة المخاطر وإستمرارية الأعمال في مواجهة الهجمات السيبرانية.

٥- فرضية الاختبارات الدورية والتقييمات: إجراء اختبارات دورية وتقييمات للأمن السيبراني يكشف الثغرات ويساعد في تحديث الإجراءات الأمنية بشكل فعال لحماية البيانات.

٦- فرضية التخطيط للطوارئ وإستعادة البيانات: وجود خطط طوارئ مفصلة وفعالة لإستعادة البيانات يقلل من تأثير الهجمات السيبرانية على إستمرارية الأعمال.



◆ الدراسات السابقة:

وجدت بعض الدراسات السابقة المتصلة بموضوع البحث أستطاع الباحث الحصول عليها وهي كالآتي:

١- دراسة (سلطان خليف ، ٢٠١٣م) بعنوان : الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني "، هدفت الدراسة الى التركيز على موضوع الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، حيث تهدف إلى تبيان مختلف التحديات والتهديدات السيبرانية التي تهدد أمن الدول، ومدى أهمية الدفاع والردع الإلكتروني لتحقيق الأمن السيبراني الوطني في ظل التحديات الراهنة، وتشير نتائج هذه الدراسة إلى أن من يمتلك القوة السيبرانية والتكنولوجيا المتقدمة ويتفرد بها سيحقق السيطرة في الفضاء السيبراني ويحقق الأمن السيبراني الذي يدعم السيادة الوطنية الكاملة للدولة.

٢- دراسة بعنوان : "إطار عمل لادارة المخاطر في مراكز البيانات لمواجهة الهجمات السيبرانية" نشرت في المجلة الدولية لأمن المعلومات والشبكات عام ٢٠٢١م، تناولت هذه الدراسة تطوير إطار عمل متكامل لتحديد المخاطر وتقييمها والتحكم بها في مراكز البيانات للحد من التأثير السلبي للهجمات السيبرانية.



٣- دراسة بعنوان: "تعزيز إستمرارية الأعمال في مراكز البيانات الحكومية:

التحديات والحلول" نشرت في مجلة الحكومة الإلكترونية عام ٢٠٢٠م، ركزت هذه الدراسة على التحديات التي تواجه إستمرارية الأعمال في المراكز الحكومية وتقديم حلول تقنية وإدارية لضمان إستمرارية الخدمات في حالة وقوع أي كوارث أو إختراقات.

٤- دراسة بعنوان: "أثر الهجمات السيبرانية على البيانات الحساسة في

المؤسسات الأهلية: دراسة حالة" نشرت في مجلة أمن تكنولوجيا المعلومات عام ٢٠١٩م، قدمت هذه الدراسة تحليلاً لحالات فقد البيانات الحساسة في بعض المؤسسات الأهلية نتيجة الهجمات السيبرانية وأوصت بتعزيز الجوانب الأمنية والرقابية.

٥- دراسة بعنوان: "دور إدارة المخاطر في تعزيز إستمرارية الأعمال في مراكز

البيانات الكبرى" نشرت في مجلة إدارة المخاطر عام ٢٠١٨. ركزت هذه الدراسة على الممارسات الفضلى لإدارة المخاطر وربطها بإستمرارية الأعمال في المراكز الكبرى لضمان إستمرارية الخدمات والحفاظ على البيانات الحساسة.

الفرق بين الدراسة الحالية والدراسات السابقة:



بعد إستعراض الدراسات السابقة التي كانت قريبة من هذا موضوع الدراسة أو متصلة بأحد جوانبه يمكن توضيح الفرق بينها وبين الدراسة الحالية في النقاط التالية:

أن الدراسات السابقة تناولت إدارة المخاطر بشكل عام، ولم تنطرق الى جوانب مختلفة لدرز مثل هذه الإدارات في الحد من الهجمات السبرانية على المنظمات الحكومية والإهلية التي تؤدي الى فقد بياناتها، كما أنها لم تشبع الموضوع بالبحث حتى في إدارة المخاطر والتي تتطلب مزيد من الدراسات، حيث تعتبر هذه الدراسة قد ركزت على موضوع ذات أهمية كبيرة.

وهناك علاقة ترابط بين الدراسات السابقة و البحث الذي بين أيدينا كونهما يتوافقان في البحث في موضوع إدارة المخاطر التي تعد العامل المشترك بينهما.

أما من حيث منهج البحث، فقد تفق هذا البحث مع بعض الدراسات السابقة في إستخدامها المنهج الوصفي التحليلي باعتباره المنهج المناسب لمثل هذه الدراسات، بينما يختلف البحث الحالي عن معظم الدراسات السابقة في إستخدام مناهج أخرى مثل المنهج الاستقرائي والمنهج المسحي والمنهج الوثائقي، وهي مختلفة عن ما تم إستخدامه في الدراسات السابقة.



أما من حيث المجتمع والعينة والأداة يختلف البحث عن الدراسات السابقة في إستهدافه لعينة بحث مختلفة عن عينة البحث الحالية، المتمثلة المنظمات الحكومية والأهلية في المملكة العربية السعودية.

◆ المنطلقات النظرية للدراسة:

تعتبر المنطلقات النظرية لهذا البحث العلمي من أهم النقاط والتي يمكن إستعراضها كالتالي:

١- نظرية إدارة المخاطر:

- أ- لتأكيد على تحديد المخاطر المحتملة والتقييم الدقيق لآثارها المحتملة.
- ب- وضع استراتيجيات فعالة للتخفيف من المخاطر والتعامل معها.
- ج- ربط إدارة المخاطر باتخاذ القرارات الإستراتيجية في منظمات القطاع الحكومي والأهلي.

٢- نظرية إستمرارية الأعمال:

- أ- التركيز على ضمان إستمرارية الخدمات والعمليات الحيوية في مواجهة الإضطرابات والكوارث.
- ب- تطوير خطط إستمرارية الأعمال والتعافي من الكوارث في مراكز البيانات.



ج- ربط إستمرارية الأعمال بتحقيق الأهداف التنظيمية وتقديم الخدمات للمستفيدين.

٣- نظرية الأمن السيبراني:

أ- التركيز على حماية البيانات والأنظمة من الهجمات السيبرانية المتطورة.

ب- وضع إجراءات وآليات فعالة للكشف عن التهديدات والتصدي لها.

ج- ربط الأمن السيبراني باستمرارية الأعمال وإدارة المخاطر في مراكز البيانات.

٤- نظرية نظم المعلومات:

أ- التركيز على دور تكنولوجيا المعلومات في دعم وتعزيز إدارة المخاطر واستمرارية الأعمال.

ب- تصميم وتنفيذ أنظمة معلومات آمنة ومرنة في مراكز البيانات.

ج- ربط نظم المعلومات بالجوانب التنظيمية والإدارية لضمان الاستخدام الأمثل.

♦ المنهجية وطرق البحث:

١- المنهج الوصفي التحليلي:

- تحليل الوضع الراهن لإدارة المخاطر وإستمرارية الأعمال في مراكز البيانات.

- وصف وتحليل التحديات والتهديدات السيبرانية التي تواجهها هذه المراكز.

- تقييم الممارسات الحالية والآثار المترتبة على فقد البيانات الحساسة.



٢- المنهج الإستقرائي:

- إستقراء الأدبيات والدراسات السابقة ذات الصلة بموضوع البحث.
- إستخلاص الدروس المستفادة والممارسات الناجحة من الحالات المماثلة.
- بناء إطار مفاهيمي شامل لدور إدارة المخاطر وإستمرارية الأعمال.

٣- المنهج الوثائقي:

- تحليل السياسات والتشريعات المنظمة لأمن المعلومات والإستمرارية في القطاعين.
 - دراسة التقارير والإحصائيات الرسمية المتعلقة بالهجمات السيبرانية وفقد البيانات.
 - استعراض الوثائق والإرشادات الفنية الصادرة عن الجهات المعنية.
- ## ٤- المنهج المسحي:

- إجراء مسح ميداني لعينة من مراكز البيانات في القطاعين الحكومي والأهلي.
- جمع البيانات والمعلومات من خلال إستبيانات وملاحظات ومقابلات.
- تحليل البيانات الكمية والنوعية لإستخلاص النتائج والتوصيات.



◆ أدوات الدراسة:

● الإستبيان:

- تصميم إستبيان شامل لجمع البيانات من مديري مراكز البيانات والأفراد المعنيين.
- تغطية محاور رئيسية مثل سياسات الأمن السيبراني، إدارة المخاطر، خطط الإستمرارية، وآليات الإستجابة للحوادث.
- تحليل النتائج الكمية والنوعية للإستبيان باستخدام أساليب إحصائية متقدمة.

● المقابلات المتعمقة:

- إجراء مقابلات شبه منظمة مع خبراء وقادة في مجال أمن المعلومات والإستمرارية.
- إستكشاف التحديات والممارسات الناجحة بشكل تفصيلي من وجهة نظر المختصين.
- تسجيل وتحليل البيانات النوعية المستقاة من المقابلات.

● ورش العمل وحلقات النقاش:

- تنظيم ورش عمل وحلقات نقاش تفاعلية مع المسؤولين في مراكز البيانات.
- مناقشة القضايا الرئيسية وتبادل الخبرات والأفكار لتطوير الحلول المناسبة.



- توثيق المناقشات وتحليل المخرجات والتوصيات الناتجة.
- تحليل الوثائق والسجلات:
- مراجعة السياسات والإجراءات الداخلية لإدارة المخاطر واستمرارية الأعمال.
- فحص سجلات الحوادث السيبرانية وإجراءات الاستجابة والتعافي.
- تحليل التقارير والإحصائيات الرسمية المتعلقة بالهجمات وفقد البيانات.
- المحاكاة والاختبارات:
- إجراء تمارين محاكاة لسيناريوهات الهجمات السيبرانية وانقطاع الخدمات.
- اختبار خطط الاستمرارية والاستعادة من الكوارث في مراكز البيانات.
- تقييم مدى جاهزية المنظمات وفعالية الإجراءات التي يتم اتخاذها.

◆ حدود الدراسة:

- النطاق الجغرافي:
- التركيز على مراكز البيانات في المنظومة الحكومية والأهلية ضمن حدود دولة المملكة العربية السعودية.
- قد يتم توسيع النطاق الجغرافي إلى مستوى إقليمي أو دولي إذا كان الهدف المقارنة بين الممارسات في مختلف الدول.
- القطاعات المستهدفة:



- التركيز على قطاعات حكومية رئيسية مثل: الصحة، التعليم، الأمن، الخدمات العامة.
- دراسة قطاعات أهلية مهمة مثل المؤسسات المالية، الشركات الكبرى، الجهات الصحية والتعليمية الخاصة.
- قد يتم توسيع نطاق القطاعات حسب أهمية البيانات المعالجة وحساسيتها.
- حجم المنظمات:
- التركيز على مراكز البيانات في المنظمات الكبرى والمتوسطة الحجم.
- قد يتم تضمين بعض المنظمات الصغيرة إذا كانت تمثل نسبة كبيرة من القطاع.
- متطلبات الأمان والإستمرارية:
- التركيز على المنظمات التي تتطلب مستويات عالية من الأمان السيبراني والإستمرارية في الأعمال.
- قد يتم إستبعاد بعض المنظمات ذات متطلبات أمنية أقل أو التي لا تتعامل مع بيانات حساسة.
- الفترة الزمنية:
- سيتم التركيز على الفترة الزمنية الحالية خلال العام الجامعي ١٤٤٦ هـ .



الفصل الثاني

الإطار النظري للبحث

المبحث الأول : إدارة المخاطر.

♦ **التعريف بمفهوم الخطر .**

♦ **التعريف بإدارة المخاطر .**

♦ **أهمية إدارة المخاطر.**

♦ **مراحل عملية إدارة المخاطر**



◆ التعريف بمفهوم الخطر:

إن كلمة خطر هي في الأصل من المصطلحات اللاتينية، ويدل على الإرتفاع في التوازن، وحدوث تغيير ما مقارنة، مع ما كان منتظرا والانحراف، المتوقع. (صوار يوسف، ٢٠٠٨م، ص ٢٣).

◆ التعريف بإدارة المخاطر:

تعرف إدارة المخاطر بأنها: الإجراءات التي تتبعها المنظمات بشكل منظم لمواجهة الأخطار المصاحبة لأنشطتها، بهدف تحقيق المزايا المستدامة من كل نشاط (آل عاض، إدارة مخاطر أمن المعلومات، د-ت، ص ٧).

هناك عدة تعاريف لإدارة المخاطر نذكر منها:

بأنها كل الإجراءات، التي تقوم بها الإدارات للعمل على الحد من الآثار السلبية الناتجة عن المخاطر، وإبقائها في الحدود الدنيا (٢٠٠٢، Catry،
(Behade, May

وتعرف إدارة المخاطر علي أنها العملية التي يتم من خلالها إدارة المؤسسة التي تستخدم عملية التعامل مع المخاطر ووضع طرق واجراءات من شأنها تقليل من إمكانية حدوث الخسائر. (المعيوفى ، وعبد العزيز، ٢٠٢٧م، ص ٥٤).



إدارة المخاطر هي عملية حيوية في أي مؤسسة، تسعى لتحديد، تقييم، والسيطرة على المخاطر التي قد تؤثر على تحقيق أهدافها. هذه العملية تشمل مجموعة من الإجراءات الاستباقية والتفاعلية التي تهدف إلى تقليل الآثار السلبية للمخاطر وتعظيم الفرص المتاحة (البحيصي، ٢٠١١م، ص ٨٧).

يمكن القول أن إدارة المخاطر يقصد بها الأساليب والعمليات التي يمكن إتباعها للتعرف على سياسات العمل وتحديد المخاطر المحتملة وفي طبيعتها طرق السيطرة عليها (عبد القادر، طمبو ولمصادفة المختار، ٢٠١٩م، ص ٩).

♦ أهمية إدارة المخاطر: (عبد الحي، ٢٠١٠م، ص ٧٢).

- ١- تحديد المخاطر والتعرف على جميع المخاطر المحتملة التي قد تواجه المؤسسة.
- ٢- تقييم المخاطر وتقدير احتمال وقوع كل خطر وتأثيره على المؤسسة.
- ٣- الإستجابة للمخاطر، ووضع خطط للتعامل مع كل خطر، مثل تجنبه، تقليله، نقله، أو قبوله.
- ٤- مراقبة وتقييم المخاطر ومتابعة فعالية خطط الإستجابة وتعديلها حسب الحاجة.



- ٥- الحفاظ على إستمرارية الأعمال، من خلال تحديد المخاطر المحتملة واتخاذ الإجراءات اللازمة لتقليل آثارها، تساعد إدارة المخاطر على ضمان إستمرارية الأعمال وتجنب التوقف المفاجئ.
- ٦- تحسين إتخاذ القرارات، من خلال توفير معلومات دقيقة حول المخاطر المرتبطة بكل قرار.
- ٧- تعزيز سمعة المنظمة، من خلال إظهار الإلتزام بإدارة المخاطر، يمكن للمنظمة تعزيز سمعتها بين العملاء والمستثمرين.
- ٨- زيادة الكفاءة، من خلال تحسين إستخدام الموارد وتقليل الهدر.
- ٩- الإمتثال للقوانين واللوائح، الذي يتطلب العديد من الصناعات والقطاعات الإمتثال لقوانين ولوائح معينة تتعلق بإدارة المخاطر.

♦ مراحل عملية إدارة المخاطر: (حاكمي، ٢٠١٤م، ص ٢٢).

- ١- تحديد المخاطر، ويتم في هذه المرحلة تحديد جميع المخاطر المحتملة التي قد تؤثر على المنظمة.
- ٢- تقييم المخاطر: و كل خطر من حيث إحتمالية حدوثه وأثرها المحتمل على المنظمة.



٣- إستجابة للمخاطر وتحديد الإستجابات المناسبة لكل خطر، مثل

تجنب الخطر، تقليل احتمالية حدوثه، تقليل تأثيره، أو تحويله إلى
جهة أخرى.

٤- المتابعة والرصد: للمخاطر بانتظام والتأكد من فعالية الإجراءات
المتخذة.

٥-



المبحث الثاني: الأمن السيبراني.

- ◆ مفهوم الأمن السيبراني.
- ◆ مجالات الأمن السيبراني.
- ◆ أهداف الأمن السيبراني
- ◆ مخاطر الهجمات السيبرانية.
- ◆ ادارة مخاطر الأمن السيبراني.
- ◆ دور إدارة المخاطر في الأمن السيبراني.
- ◆ طرق تعزيز الأمن السيبراني.



◆ مفهوم الأمن السيبراني:

يمكن القول بأن الأمن السيبراني، يتمثل في عملية الحماية للأنظمة والبيانات والشبكات والبرامج، ضد الهجمات الالكترونية، وذلك الأمن يحتوي على طبقات متعددة من حماية قوية تنتشر في أجهزة الحاسوب الآلي والشبكات والبرامج والبيانات، التي يريد الشخص حمايتها والإحتفاظ بها سواء على المستوى الفردي أو على المستوى المؤسسي، وتتمثل الهجمات السيبرانية بالمحاولات المتعددة التي تصدر من قبل الافراد أو المؤسسات لاختراق نظام المعلومات لدى فرد أو مؤسسة أخرى، لهذا إن الأمن السبراني يتمثل في: جميع التدابير والإجراءات والأدوات والتقنيات التي يتم استخدامها لحماية وسلامة الشبكات والبرامج والبيانات من الهجوم، أو الوصول غير المسموح، أو الإتلاف، كما يشمل حماية الأجهزة المادية، والقواعد البيانية(السمحاني، ٢٠٢٠م، ص٤٣).

وكذلك يعرف بأنه : الممارسة القوية للدفاع عن أجهزة الحاسب الالي، والخوادم، والأجهزة المادية، المحموله والانظمة الالكترونية والشبكات، والبيانات، من الهجوم الضار(عبد الجواد، ٢٠٢٠م، ص٩٧).



♦ مجالات الأمن السيبراني: (البردان و شحاتة، ٢٠٢١م، ص ١١).

- هناك ستة مجالات عامة يمكن تضمينها في الأمن السبراني، وهي كالآتي:
- التأمين الشبكات، ممارسة تأمين الشبكات للحاسب الآلي من أي تطفل، سواء كانوا مهاجمين مستهدفين، أو برامج إنتهازية ضارة.
 - التأمين للتطبيقات، يمكن من خلال ذلك إن يوفر التطبيق المخترق الوصول الى البيانات المصممة لحمايتها، ويبدأ الأمان الناجح في مرحلة التصميم قبل نشر البرنامج أو الجهاز بوقت طويل.
 - أمن المعلومات سلامة وخصوصية البيانات: سواء عند النقل أو أثناء عملية التخزين.
 - الأمن التشغيلي العمليات والقرارات الخاصة بمعالجة أصول البيانات والحماية لها، أي الأذونات التي يمتلكها المستخدمون عند الوصول الى الشبكة والإجراءات التي تحدد كيف وأين يمكن تخزين البيانات أو مشاركتها كلها تندرج تحت هذه المظلة.
 - تعزيز تعافي المؤسسات من الهجمات الإلكترونية بأشكالها المختلفة، يحدد التعافي من الكوارث، وإستمرارية الأعمال كيفية إستجابة المنظمة لحوادث مخاطر الهجمات السيبرانية، أو أي حدث آخر يتسبب في فقدان العمليات أو البيانات، ومن ثم تملئ سياسات التعافي من الكوارث، كيفية استعادة



المؤسسة لعملياتها، ومعلوماتها للعودة الى نفس القدرة التشغيلية، كما كانت قبل الحدث وبالتالي إستمرارية العمل هي الخطة التي تعود عليها المنظمة أثناء محاولتها العمل بدون موارد معينة.

- تدريب المستخدم النهائي الأشخاص أكثر عوامل مخاطر الهجمات السيبرانية التي لا يمكن التنبؤ بها: حيث يمكن لأي شخص إدخال فيروس بطريق الخطأ إلى نظام آمن من خلال عدم إتباع ممارسات الأمان الجيدة ويعد تدريب المستخدمين حذف مرفقات البريد الإلكتروني المشبوهة، وليس توصيل محركات أقراص يو إس بي غير محددة الهوية، والعديد من الدروس المهمة الأخرى أمراً حيوياً لأمن أي مؤسسة.

◆ أهداف الأمن السيبراني:

يمكن القول أن أهم أهداف الأمن السيبراني تتمثل في الآتي: (عماد الدين،

٢٠٢٣م، ص ٥٥)

- تمكين الحماية لأنظمة التقنيات التشغيلية، في كافة المجالات، ومكوناتها، من الأجهزة والبرمجيات، وخدماتها وما تحتوي من البيانات.



- التصدي والمواجهة للهجمات، والحوادث التي تحدث نتيجة، مخاطر الهجمات السيبرانية، التي يتم من خلالها إستهداف الأجهزة الحكومية، والمؤسسات في القطاع العام والأهلي.
- العمل على توفير البيئة الآمنة الموثوقة التعاملات، في المجتمع المعلوماتي، وعصر التكنولوجيا الرقمية.
- جعل البنى التحتية، الأكثر حساسية من الهجمات الإلكترونية، أكثر صموداً.
- الحد من المخاطر والجرائم السيبرانية، التي يتم من خلالها إستهداف المستخدم، وذلك من خلال توفير المتطلبات اللازمة.
- معرفة النقاط الضعيفة في أنظمة الحاسب الآلي، والأجهزة المحمولة، المختلفة.
- معالجة سد الثغرات، في الأنظمة المعلوماتية.
- المقاومة للبرمجيات الضارة، التي تهدف الى إحداث الأضرار البالغة للمستخدم.
- منع التخريب والتجسس الإلكتروني، على المستوى الفردي أو الحكومي.
- العمل على إتخاذ التدابير اللازمة، للمستهلكين على حد سواء، من أي مخاطر محتملة في المجالات المستخدمة في الإنترنت.



- التدريب للأفراد على الإجراءات والآليات الجديدة، لمواجهة التحديات الخاصة بإختراق الاجهزة التقنية، بغرض الضرر بالمعلومات الشخصية.

◆ مخاطر الهجمات السيبرانية:

إن الهجمات السيبرانية مع مرور الأيام في تزايد، وتظهر الجرائم الإلكترونية بأشكال متنوعة، ومختلفة، وذلك بإعتماد المجرم على العديد من التقنيات، التي تستخدم في الجرائم، لا يقتصر التأثير للجرائم الالكترونية على الضحايا فقط، لكن تأثيرها يمتد على كامل المجتمع، وتتمثل عواقب جرائم الإللكترونية على الإقتصاد، في ضياع الوقت، فقدان الإيرادات، والإنتاجية المنخفضة، وتلف السمعة، وغيرها من العواقب (برادة، ٢٠٢٤م، ص ١٠).

ومن المخاطر التي تنتج عن التقنيات الإختراق السيبراني لمؤسسات الدولة الحكومية والأهلية، وأفرادها والأثر الكبير الذي يحدثه التطور العلمي في مجال برمجة المعلومات وهي كالاتي: (Conteh & Schmick, 2021)

- المخاطر في تأمين البيانات والمعلومات، تسهل تكنولوجيا الإنترنت على جمع كميات كبيرة من البيانات وتخزينها، ويمكن أن تكون عبارة عن معلومات خاصة، تتعلق العاملين، أو المؤسسات، وقد يكون من الصعب، الحفاظ



على الأمان لهذه البيانات، فعند اخراق واحد، يمكن الوصول الى كميات كبيرة من المعلومات الخاصة، إلى يد المجرمين، أو المنافسين، أو الخصوم، الأجانب.

- إنتهاك الخصوصية، ويعتبر الحفاظ على الخصوصيات الشخصية في المجال الرقمي الأكثر صعوبة، في ظل التزايد لمخاطر سرقة البيانات الشخصية، أو الإبتزاز عبرها.

- إنتهاك حقوق الملكية الفكرية، في ظل العصر التكنولوجي، حيث أصبح الأمر سهلا في نسخ الوسائط الرقمية، وإعادة الإنتاج لها، ويكون من الصعوبة تطبيق قوانين حقوق النشر.

- عدم الكشف عن الهوية، حيث توفر تكنولوجيا الإنترنت المجال الواسع للمستخدم لإخفاء هويته، كما تشير إليه كثير من الدراسات على أنه من المرجح، أن يتصرف المستخدم بشكل عدائي لمجتمعه، لاعتقادهم بعدم وجود أي عواقب وعقوبات.

- إنعدام الإيرادات، من التأثير للجرائم الإلكترونية على الإقتصاد بشكل عام هو إنعدام الإيرادات، الذي يمكن أن يستتب إنعدام الإيرادات، وذلك نتيجة التسريب للمعلومات المالية الحساسة من قبل الطرف المهاجم عند الحصول عليها، والتي يتم استخدامها من قبله لسحب الأموال من حسابات هذه المؤسسات، ويمكن أن تتم الجرائم الالكترونية، عند اختراق أي موقع تجاري



إلكتروني، خاص بأي شركات، ويصبح غير قابل للتشغيل من قبل المؤسسة، لذلك ينعدم الدخل القيم، يضيع في حالة عدم قدرة المستهلكين، استخدام الموقع، مما يؤدي الى خسائر على المؤسسات.

- الأضرار بسمعة المؤسسات الحكومية والأهلية، في الحالات التي يتم فيها الهجوم الإختراقي، للمؤسسات مثل البنوك وغيرها، الامر الذي يعرض بيانات العملاء ، للمؤسسات الى الإختراق الأمني، مما يؤثر هذا نوع من الجرائم، على سمعة المؤسسات، وذلك لأن نظامها، وبنيتها المعلوماتية، غير آمنة، وهي في خطر من طرف القراصنة أو المتسللين، أو أي مجرم إلكتروني، يؤدي الى فقدان الثقة في المؤسسة، حيث يعملون على تغييرها بمؤسسات أخرى، لديها الحماية الأفضل والكافية لممتلكات العملاء، مما يسبب لها الخسارة المادية والتشويه لسمعة المؤسسات.

- الإنخفاض في الإنتاجية، حيث يتوجب على المؤسسات، ذات الأنشطة الإقتصادية والمالية، الى العمل على اتخاذ جملة إجراءات، تعمل على مكافحة الجرائم الالكترونية، في الغالب يكون هناك التأثير السلبي لها على الإنتاجية، وعلى عمل الموظفين وأدائهم. (دانيال ايجا وآخرون ٢٠١٨م، ص ١٥٦).

♦ ادارة مخاطر الأمن السيبراني:

إن المؤسسات الأهلية، والحكومية، وبالأخص الإقتصادية المالية، تعد من الأهداف الجذابة وبشكل متزايد، من قبل الهجمات السيبرانية، كما تعمل الدول المتقدمة، على تعزيز الدفاعات الإلكترونية، إن الانتشار الخدمات الرقمية، أدى إلى تفاقم التهديدات التي تشكلها الهجمات السيبرانية، على المنشآت الرقمية الحكومية والأهلية في البلدان النامية، التي ليس لها دفاعات قوية، إن بناء الدفاع القوي على الإنترنت من الأمور بالغت الأهمية، البيانات وتأمينها، يمكن للهجمات الالكترونية، أن تثبط الجهود الشمول المالي لأنها، إذا نجحت، فقد تخوف العملاء من تبني المنتجات والخدمات المعتمدة على التقنية الرقمية. (بن علية بن جدو، ٢٠٢٢م، ص ٣٠٤).

♦ دور إدارة المخاطر في الأمن السيبراني والحد من الجريمة

الإلكترونية:

تعمل المؤسسات، من خلال إدارة المخاطر والإطار الأمني لها، على تحقيق البيئة المستقرة، والعمل على توفير الشروط التي تتكيف معها المؤسسة في التنظيم المناسب لها، ويرجع هذا الى لمهام الرئيسية التي تتمثل في الإنتاج ، وهي التي



تتعرض لمشاكل متنوعة، في الجانب الأمني السيبراني، مثل السرقة الملكية، الفكرية، وسرقة الخصوصيات الطلاب، والموظفين، إضافة الى الإختراق للبوابات الرقمية المعتمدة طرفها، وذلك من المشاكل التي توجهها كل المؤسسات، الحكومية والأهلية ومن الأهداف الرئيسة في عمل إدارة المخاطر :

- التعليم، وذلك من خلال العمل على إنشاء البيئة التعليمية للطلاب والأساتذة، وعقد الملتقيات، والمحاضرات، التي تتناول المواضيع المتعلقة بالسلامة، والأمن، عند الإستخدام للأنترانت، وكذلك حول الأساسيات في الأمن السيبراني، والحفاظ علي البيانات، والتواصل من خلال الإستخدام بمواقع التواصل الإجتماعي وحمايتها. (Chou, C., & Peng, H. 2011).

- العمل على تحديد التهديدات الإلكترونية، في هذا الإطار الذي تعمل عليه إدارة المخاطر وفي الجانب الأمني السيبراني، هو التحديد الدقيق للتهديدات السبرانية، التي يحتمل أن تتعرض لها المؤسسات، والتي تعتبر من التحديات التي أصبحت تشهدها المؤسسات، أو التي ينفذها المجرمين على الأنترانت، والتي تتمثل بأنشاء الموقع المزيفة على الويب للمؤسسات، بغرض الاحتيال، وكذلك تحديد التهديدات المحتملة، التي يمكن أن تسير كل الظروف



والمشاكل يحتمل أن تعرقل عمل هذه المؤسسات، قبل حدوثها وهذا يدخل في جانب التنبؤ بالمخاطر (لسعيري، ٢٠١٩م، ص ٢٩٨).

- البناء للبرنامج الأمني: من خلال برنامج الأمن السيبراني الذي تبنه الإدارة على المدى القريب والبعيد لتقليل من ضعف نظامها، وشبكاتها التي تعمل في الفضاء الإلكتروني والذي يتماشى مع قدراتها المادية والتقنية والبشرية، في المواجهة (عوفي، ٢٠٢٢، ص ٩٨).

♦ طرق تعزيز الأمن السيبراني:

يتكون تعزيز الأمن السبراني من الخطوات الآتية: (الهزاني، ٢٠٢٣م، ص ٨١)

- إدارة أصول البيانات للمنظمة: يجب التأكد أن الجهة، التي تملك قائمة الجرد الدقيقة والحديثة للأصول أنها في آمان، وذلك لدعم عمليات تشغيل الجهة وما يتطلبه الأمن السيبراني، وذلك لتحقيق السرية للأصول للبيانات، والتقنيات، للجهة من أجل سلامتها، وتوافرها ودقتها.

- هويات الدخول، والصلاحيات، وإدارتها، من أجل ضمان حماية الأمن للبيانات، والوصول المنطقي، إلى أصول المعلومات والتقنيات للمنظمة، والعمل على منع أي وصول غير مشروع.



- الحماية للأنظمة والأجهزة الخاصة بمعالجة المعلومات، ان ضمان الحماية للأنظمة والأجهزة الخاصة بمعالجة المعلومات، بما فيها أجهزة المستخدمين، والبنية التحتية، للمنظمة من إي مخاطر سيبرانية.
- تأمين الأجهزة المحمولة، من اجل حماية الأجهزة المحمولة لأي منظمة، من مخاطر الهجمات السيبرانية، والتعامل بشكل أكثر أمانا مع المعلومات الحساسة، والمعلومات الخاصة، بالأعمال التابعة للمنظمة، والحماية لها أثناء النقل، والتخزين، في حال استخدام الأجهزة الشخصية، للعاملين في المنظمة.
- الحماية التامة للبيانات والمعلومات، أن حماية البيانات السرية، وسلامة بياناتها، والمعلومات الخاصة بالجهة ودقتها، وتوافرها.
- الإدارة لسجلات الأحداث، والمراقبة الدقيقة للأمن السيبراني، لتجميع السجلات وأمنها السيبراني، ومراقبتها، وتحليلها، في الوقت المناسب، لابد من الإكتشاف الإستباقي، لأي هجوم سيبراني، وإدارة المخاطر، والعمل على المنع أو التقليل من الآثار المترتبة عليها، في أعمال المنظمة.
- تهديدات الأمن السيبراني، وأدارة حوادثها، لابد من التحديد والإكتشاف لحوادث الأمن السيبراني، في الوقت المبكر، والإدارة لها بشكل فعال، والتعامل مع التهديدات السيبرانية قبل وقوعها.



الفصل الثالث

منهجية وإجراءات الدراسة

- ◆ منهج الدراسة .
- ◆ مجتمع الدراسة.
- ◆ عينة الدراسة .
- ◆ أداة الدراسة .
- ◆ — صدق الأداة.
- ◆ — ثبات الأداة.
- ◆ إجراءات الدراسة.
- ◆ متغيرات الدراسة.



◆ منهج الدراسة:

تعد منهجية الدراسة الركن الأساسي في تصميم البحث لأنه الخطة التي تحتوي على الطريقة والتي من خلالها يتم تحديد المفاهيم والمعاني الإجرائية، وأداة جمع البيانات، وتحديد مجتمع الدراسة ومجالاتها.

تم استخدام المنهج الوصفي المسحي التحليلي، في هذه الدراسة الذي يعمل على وصف الظواهر، والأحداث موضوع الدراسة، وكذلك إستخدام منهج دراسة الحالة الذي يعد من أنسب المناهج لمثل هذه البحوث، لما يوفره من بيانات دقيقة وتفصيلية، عن الحالات موضوع الدراسة ولما لائمته الدراسات الإستراتيجية، وكذلك استخدم أسلوب المقارنة، كما استخدم أسلوب التحليل الإحصائي، وتحديدًا لتحليل البيانات واختبار فروض البحث. يهدف أسلوب دراسة الحالة برنامج (SPSS) إلى التعرف على خصائص ومضمون حالة أو ظاهرة واحدة أو مجموعة حالات أو ظواهر بصورة مفصلة ودقيقة، ثم جمع معلومات مفصلة ودقيقة عنها وتحليل البيانات والمعلومات التي تم جمعها بطريقة علمية وموضوعية للحصول على نتائج محددة يمكن تعميمها واقتراح أساليب معالجتها على حالات أخرى مشابهة.



◆ مجتمع الدراسة:

يعرف مجتمع الدراسة بأنه جميع مفردات الظاهرة التي يدرسها الباحث، وبناءً على مشكلة الدراسة وأهدافها فإن المجتمع المستهدف مجتمع البحث يتكون من عينة عشوائية تمثلت في المنظمات الحكومية والأهلية في المملكة العربية السعودية.

◆ عينة الدراسة:

قام الباحث باستخدام أسلوب إختيار العينة العشوائية في الدراسة، أما عن عينة الدراسة فقد تكونت من جميع العاملين في المنظمات الحكومية والأهلية في المملكة العربية السعودية، ونظرا لكبر العينة فقد تم اختيار العينة بشكل عشوائي من كل العاملين في المنظمات الحكومية والاهلية في المملكة العربية السعودية.

وعينة الدراسة مكونة قام الباحث بإختيار عينة الدراسة بطريقة عشوائية قام الباحث باختيار عينة الدراسة بطريقة عشوائية من العاملين في المنظمات الحكومية المختلفة في المملكة العربية السعودية، والذين بلغ عددهم (٥٠) فردًا.



◆ أداة الدراسة:

استخدمت الدراسة أداة الاستبانة لجمع البيانات لكونها من أفضل الأدوات مناسبة لهذا النوع من الدراسات، والتي سيتم تفصيلها بشكل معمق من خلال الدراسة العملية.

- **الهدف العام من الاستبيان** قام الباحث بإعداد أداة الدراسة (الاستبيان) لمعرفة " التعرف على دور إدارة المخاطر واستمرارية أعمالها في مراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية " وأتبع الباحث الخطوات التالية لبناء الإستبانة:

- ١- الإطلاع على الأدبيات النظرية والدراسات السابقة ذات الصلة بموضوع الدراسة، والإستفادة منها في بناء الإستبانة وصياغة فقراتها.
- ٢- إستشار الباحث عدداً من أساتذة الجامعات والمشرفين في تحديد أقسام الاستبانة وأسئلتها.
- ٣- تحديد الأقسام الرئيسة التي شملتها الاستبانة.
- ٤- تحديد الأسئلة التي تقع تحت كل قسم.
- ٥- تم تصميم الاستبانة في صورتها الأولية.
- ٦- تم مراجعة وتنقيح الاستبانة من قبل المشرفين.
- **مفتاح تصحيح الاستبيان:** أعتمد الباحث بالاستبيان على مقياس ليكرت المتدرج والمكون من خمس درجات، لقياس البنود المختلفة، ويأخذ هذا



المقياس بالشكل التالي: (موافق بشدة=٥، موافق=٤، محايد=٣، غير موافق=٢، غير موافق بشدة=١).

- محتوى الاستبيان:

يتضمن الاستبيان على جزئين، وهما كما يلي:

الجزء الأول: البيانات الديمغرافية وهي (الجنس، عدد سنوات الخبرة، المؤهل العلمي).

الجزء الثاني: محاور الاستبيان، وهما:

- المحور الأول: (تقييم إجراءات إدارة المخاطر السيبرانية) ويتضمن هذا المحور على ٥ فقرات.

- المحور الثاني: (تقييم خطط استمرارية الأعمال) ويتضمن هذا المحور على (٤) فقرة.

- المحور الثاني: (تقييم حماية البيانات الحساسة) ويتضمن هذا المحور على (٥) فقرة.



- صدق الأداة:

• الصدق الظاهري:

يقوم مقياس صدق المحتوى على ربط الإستبانة بأهداف الدراسة، ويعتبر هو نوع من أنواع الصدق الظاهري وذلك لأنه يعكس قدرة فقرات الإستبانة على تغطية المجال الذي ينتمي إليه وعادة يتم عرض الاستبانة على مجموعة من الخبراء الأكاديميين في المجال، فبعد تصميم أداة البحث بصيغتها الأولية، تم عرضها على عدد من المحكمين من ذوي الخبرة والمعرفة في مجال الإحصاء والتربية والبحث العلمي، من أعضاء هيئة التدريس والمختصين في عدد من الجامعات، وذلك للاستفادة من خبراتهم في اختصاصاتهم والتأكد من وضوح وصلاحيه فقرات الإستبانة، وتم الطلب منهم إبداء آرائهم في مدى مناسبة العبارات لقياس ما وضعت لأجله، وقد تم الأخذ بملاحظات ومقترحات المحكمين في إعادة صياغة بعض الفقرات وحذف البعض، وإضافة بعض الفقرات في ضوء المقترحات المقدمة، وهذا بعد مناقشة المشرف وأخذ رأيه وموافقة، وبذلك خرجت الاستبانة بصورتها النهائية.

• صدق الاتساق الداخلي:

يقصد بثبات الإستبانة أن تعطي هذه الإستبانة نفس النتيجة لو تم إعادة توزيع الإستبانة أكثر من مرة تحت نفس الظروف والشروط، أو بعبارة أخرى أن



ثبات الإستبانة يعني الإستقرار في نتائج الإستبانة وعدم تغييرها بشكل كبير فيما لو تم إعادة توزيعها على أفراد العينة عدة مرات خلال فترات زمنية معينة.

بعد التأكد من صدق المحكمين لأداة الدراسة قامت الباحثة بحساب معامل إرتباط بيرسون لمعرفة الاتساق الداخلي للأداة حيث تم حساب معامل الارتباط بين درجة كل محور من محاور الاستبيان مع الدرجة الكلية للاستبيان الذي ينتمي إليه كما في الجدول التالي:

قام الباحث بإجراء اختبار بيرسون للتأكد من صدق محاور الاستبيان، وهي كما بالجدول التالي:

جدول ١ معامل إرتباط بيرسون لمحاور الإستبيان

المحاور	معامل الارتباط سبيرمان	القيمة الاحتمالية (Sig)
تقييم إجراءات إدارة المخاطر السيبرانية	**٠.٩٠٦	.000
تقييم خطط استمرارية الأعمال	**٠.٧٧٦	.000
تقييم حماية البيانات الحساسة	**٠.٨٤٧	.000

(**) تعني وجود علاقة ذات دلالة إحصائية عند مستوى دلالة (٠.٠١)

فأقل.



ويتضح من الجدول السابق أن جميع معاملات الارتباطات لمحاور الاستبيان جاءت دالة إحصائياً؛ لأن مستوى الدلالة بها جاء أقل من ٠.٠٥، كما جاء جميع محاور الاستبيان بقيمة ارتباط عالية جداً، فكانت جميع القيم أكبر من ٠.٣٠، مما يدل أن جميع المحاور مترتبة بشكل كبير مع الاستبيان، ولا يمكن حذف أي محور من محاوره.

ثبات أداة الدراسة:

أعتمد الباحث على معامل ألفا كرونباخ (Crenpach's Alpha)، وذلك للتأكد من صلاحية الاستبانة كأداة لجمع البيانات اللازمة للدراسة الحالية وأنها تقيس ما يجب قياسه، والجدول التالي يوضح معاملات ألفا كرونباخ لجميع متغيرات الدراسة، كما يلي:

جدول ٢ قيم معاملات ألفا كرونباخ لأداة الدراسة.

المحور	عدد الفقرات	معامل ألفا كرونباخ
تقييم إجراءات إدارة المخاطر السببرانية	٥	٠.٨٤٣
تقييم خطط استمرارية الأعمال	٤	٠.٨٠٨
تقييم حماية البيانات الحساسة	٥	٠.٨٤٠



يتضح من الجدول السابق أن جميع معاملات ألفا كرونباخ لكافة متغيرات الدراسة كانت أكبر من ٧٠٪، وهذا يشير إلى أن جميع الفقرات التي تم استخدامها في قياس متغيرات الدراسة ذات موثوقية عالية، بينما جاء الثبات العام للاستبيان بمقدار (٠.٨٢٦) والذي جاء بمقدار عالي جداً من الثبات.

◆ فروض الدراسة:

الفرضية الأولى: يوجد أثر ذو دلالة إحصائية لتقييم إجراءات إدارة المخاطر السيبرانية في المراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية.

الفرضية الثانية: يوجد أثر ذو دلالة إحصائية لخطط استمرارية الأعمال في المراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية.



الفرضية الثالثة: يوجد أثر ذو دلالة إحصائية لتقييم حماية البيانات الحساسة في المراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية.

الفرضية الرابعة: توجد فروض ذات دلالة إحصائية لدور إدارة المخاطر واستمرارية أعمالها في المراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية تعزي لمتغير النوع والخبرة والمؤهل العلمي.

◆ الاساليب الإحصائية المستخدمة:

قبل أن يقوم الباحث بتحديد الأساليب الإحصائية لهذه الدراسة قامت بإجراء اختبار اعتدالية البيانات لتحديد طبيعة البيانات المستخدمة في هذه الدراسة، والتي من خلالها ستمكن من تحديد الأساليب الإحصائية التي سيتم استخدامها بهذه الدراسة، لذلك قام الباحث بإجراء اختبار التوزيع الطبيعي للبيانات وهو Kolmogorov-Smirnov & Shapiro-Wilk، بالجدول التالي:

البُعد			
Shapiro-Wilk		Kolmogorov-Smirnov	
.Sig	Statistic	.Sig	Statistic



٠.١٤٣	٠.٢٠٩	٠.٩١٧	٠.٢٠٠	تقييم إجراءات إدارة المخاطر السيبرانية
٠.١٥٥	٠.٣٢٣	٠.٩٠٢	٠.١٢٠	تقييم خطط استمرارية الأعمال
٠.١٢٩	٠.٢٣١	٠.٩٢١	٠.١٠٩	تقييم حماية البيانات الحساسة

ويتضح من الجدول السابق أن البيانات معلميه وتتبع التوزيع الطبيعي للبيانات، وبناءً على ذلك سيتم استخدام الأساليب الإحصائية التالية:

- الإحصاءات الوصفية (التكرارات والنسب المئوية).
- اختبار بيرسون pearson لقياس صدق أداة الدراسة.
- اختبار ألفا كرونباخ Cronbach's Alpha، لقياس الثبات العام لأداة الدراسة.
- معامل الانحدار الخطي البسيط لقياس مدى الأثر بين متغيرات الدراسة.
- اختبار T-test وتحليل التباين الأحادي One Way ANOVA، لقياس دلالة الفروق بين متغيرات الدراسة.

◆ إجراءات الدراسة.



- قام الباحث بتناول الإطار النظري والدراسات السابقة لتغطية كافة الجوانب المتعلقة بالمتغيرات الذي سوف يتناولها الدراسة.
- عمل الباحث على تحكيم استبيان الدراسة من قبل المختصين ليتم توزيعها على المبحوثين بصورتها النهائية.
- ثم توزيع الاستبانة على المبحوثين ثم جمع كافة النسخ الموزعة من هذه الاستبانات لتم ترميزها وتفرغها ضمن البرنامج الإحصائي المناسب.
- ثم إدخال وترميز الاستبانات للشروع في عملية تحليلها.
- ثم إجراء التحليل الإحصائي لاختبار فرضيات الدراسة.
- ثم مناقشة النتائج وكتابة التوصيات التي تخدم الدراسات التالية في نفس المجال.



الفصل الرابع

الجانب العملي

- ◆ تحليل وعرض نتائج الدراسة ومناقشتها.
- تحليل البيانات الديمغرافية لعينة الدراسة.
- تحليل محتويات الاستبيان.
- ◆ النتائج والتوصيات.



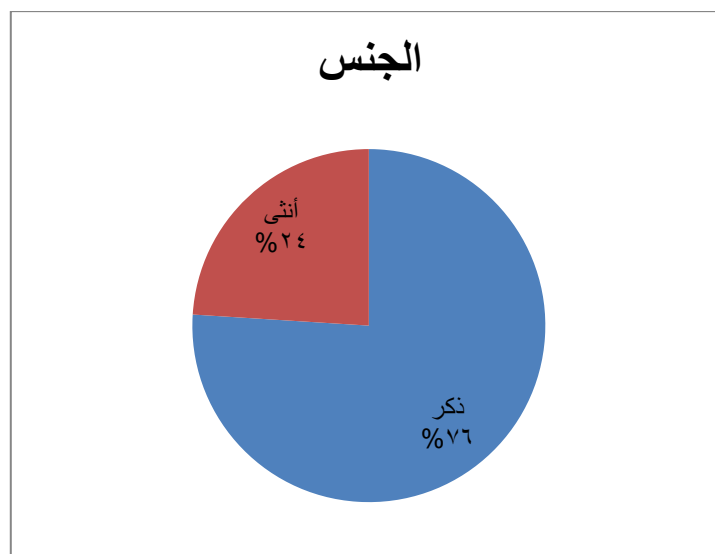
◆ تحليل البيانات الديمغرافية لعينة الدراسة.

- النوع:

جدول ٣ خصائص عينة الدراسة وفقاً لمتغير النوع.

النوع	التكرار	النسبة المئوية
ذكر	٣٨	٧٦%
أنثى	١٢	٢٤%
المجموع	٥٠	١٠٠%

يتضح من الجدول السابق أن نسبة الذكور جاءت أعلى من نسبة الإناث، حيث جاءت نسبة الذكور بمقدار (٧٦%)، بينما جاءت نسبة الإناث بمقدار (٢٤%).





شكل ١ توضيح خصائص عينة الدراسة وفقاً لمتغير الجنس.

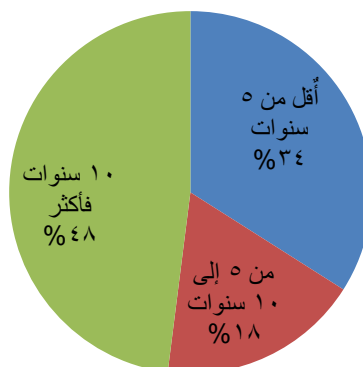
- عدد سنوات الخبرة:

جدول ٤ توزيع خصائص عينة الدراسة وفقاً لمتغير عدد سنوات الخبرة

عدد سنوات الخبرة	التكرار	النسبة المئوية
أقل من ٥ سنوات	١٧	٣٤%
من ٥ إلى ١٠ سنوات	٩	١٨%
١٠ سنوات فأكثر	٢٤	٤٨%
المجموع	٥٠	١٠٠%

يتضح من الجدول السابق أن نسبة (٤٨%) من أفراد عينة الدراسة كان مستوى الخبرة لديهم ١٠ سنوات فأكثر، بينما جاءت نسبة (٣٤%) من أفراد عينة الدراسة عدد سنوات خبرتهم أقل من ٥ سنوات، وأخيراً جاءت نسبة (١٨%) من أفراد عينة الدراسة عدد سنوات خبرتهم من ٥ إلى ١٠ سنوات.

عدد سنوات الخبرة



شكل ٢ توزيع خصائص عينة الدراسة وفقاً لمتغير عدد سنوات الخبرة.

– المؤهل العلمي:

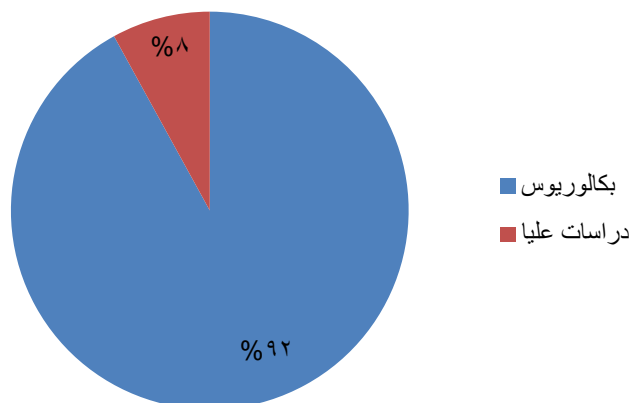
المستوى التعليمي	التكرار	النسبة المئوية
بكالوريوس	٤٦	٩٢%
دراسات عليا	٤	٨%
المجموع	٥٠	١٠٠%

يتضح من خلال الجدول السابق أن نسبة (٩٢%) من أفراد عينة الدراسة

كان مؤهلهم العلمي بكالوريوس، بينما جاءت نسبة (٨%) من أفراد عينة

الدراسة كان مؤهلهم العلمي دراسات عليا.

المرهل العلمي



شكل ٣ توزيع خصائص عينة الدراسة وفقاً لمتغير المؤهل العلمي



◆ تحليل محتويات الاستبيان:

أولاً: تقييم إجراءات إدارة المخاطر السيبرانية.

جدول ٥ المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة

الدراسة عن المحور الأول.

رقم	الفقرات	المتوسط الحسابي	الانحرافات المعيارية
١	تقوم مؤسستكم بتقييم المخاطر السيبرانية بشكل دوري.	٤.٢٠٠	٠.٧٢٨٤
٢	يتم تحديد المخاطر السيبرانية الأكثر احتمالاً وخطورة على مؤسستكم .	٤.٣٤٠	٠.٦٢٦٢
٣	يتم وضع خطط استجابة للطوارئ لمواجهة الهجمات السيبرانية .	٤.١٠٠	٠.٦٧٧٦
٤	يتدرب الموظفون بانتظام على كيفية التعامل مع تهديدات الأمن السيبراني .	٤.٢٨٠	٠.٥٧٢٨
٥	يتم تحديث برامج الحماية والأمن بشكل دوري	٤.٢٠٠	٠.٧٥٥٩



المحور ككل	٤.٢٢٤	٠.٤٢٣١
------------	-------	--------

يبين الجدول السابق أن المتوسطات الحسابية لمحور تقييم المخاطر السلوكية المرتبطة باتخاذ القرارات تراوحت ما بين (٤.١٠٠-٤.٢٠٠) وإن إجمالي البُعد (٤.٢٢٤) بأهمية عالية.

ثانياً: تقييم خطط استمرارية الأعمال.

جدول ٦ المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة عن المحور الثاني

رقم	الفقرات	المتوسط الحسابي	الانحرافات المعيارية
١	لدى منظمتك خطة واضحة لاستمرارية الأعمال في حالة حدوث حادث سيبراني .	4.0400	.63760
٢	يتم إختبار خطة استمرارية الأعمال بشكل دوري .	4.4200	.64175
٣	يتم تحديث خطة استمرارية الأعمال بشكل دوري.	4.3800	.66670
٤	تخزن منظمتك نسخ إحتياطية من البيانات بشكل منتظم	4.5200	.64650



المحور ككل	٤.٣٤٠٠	٠.٤١٢٦
------------	--------	--------

يبين الجدول السابق أن المتوسطات الحسابية لمحور دور الابتكار في تقليل المخاطر السلوكية تراوحت ما بين (٤.٠٩١-٤.٣٠٩) وإن إجمالي البُعد (٤.٢١٦) بأهمية عالية.

ثالثاً: تقييم حماية البيانات الحساسة.

جدول ٧ المتوسطات الحسابية والانحرافات المعيارية لاستجابات أفراد عينة الدراسة عن المحور الثالث.

رقم	الفقرات	المتوسط الحسابي	الانحرافات المعيارية
١	تشفر البيانات الحساسة المخزنة في مركز البيانات	4.5800	.53795
٢	تعمل المنظمة على التحقق من هوية المستخدمين قبل منحهم الوصول إلى البيانات الحساسة .	4.1600	.76559
٣	المراقبة للنشاطات المشبوهة في النظام بشكل مستمر .	4.4000	.67006
٤	يتم إجراء تدقيق داخلي وخارجي على إجراءات أمن المعلومات بشكل دوري .	4.4000	.57143
٥	يتم إبلاغ الجهات المختصة في حال حدوث أي اختراق أمني	4.2200	.88733



المحور ككل	4.3520	٠.٤٣٦٢
------------	--------	--------

يبين الجدول السابق أن المتوسطات الحسابية لمحور دور شركة سابك في تشجيع الابتكار وتقليل المخاطر السلوكية تراوحت ما بين (٤.١٦٠) - (٤.٢٢٠) وإن إجمالي البُعد (٤.٣٥٢٠) بأهمية عالية.

♦ التحقق من فرضيات الدراسة.

-الفرضية الأولى:

والتي تنص على أنه: "يوجد أثر ذو دلالة إحصائية لتقييم إجراءات إدارة المخاطر السيبرانية في المراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية"، وللتأكد من صدق هذه الفرضية قام الباحث بإجراء اختبار الانحدار الخطي البسيط، وذلك وفقاً للجدول التالي:

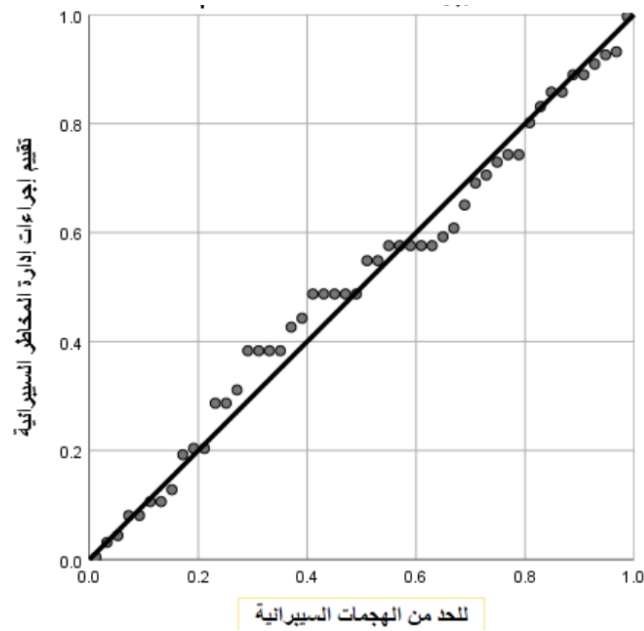
جدول ٨ نتائج تحليل الانحدار الخطي البسيط للفرضية الأولى.

تقييم	قيمة R	قيمة R2	قيمة B	قيمة (T)	Sig.
إجراءات					
إدارة					
المخاطر					



للحد من الهجمات السيبرانية	٠.٩٠٦	٠.٨٢٠	١.٠٦٣	١٤.٧٩٠	٠.٠٠٠
----------------------------------	-------	-------	-------	--------	-------

يتضح من خلال الجدول السابق أن معامل الانحدار الخطي البسيط للفرضية الأولى يساوي (٠.٩٠٦)، وأن قيمة الارتباط بين أثر تقييم إجراءات إدارة المخاطر السيبرانية للحد من الهجمات السيبرانية في المملكة العربية السعودية، جاء بمقدار (١٤.٧٩٠)، وجاء بمستوى دلالة (٠.٠٠٠) وكان أقل من (٠.٠٥) مما يدل على أنه دال إحصائيًا، لذلك نرفض الفرض الصفري ونقبل بالفرض البديل والذي ينص على أنه: "يوجد أثر ذو دلالة إحصائية لتقييم إجراءات إدارة المخاطر السيبرانية في المراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية".



شكل ٤ الانحدار الخطي للفرضية الأولى.

—الفرضية الثانية:

والتي تنص على أنه: "يوجد أثر ذو دلالة إحصائية لخطط استمرارية الأعمال في المراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية"، وللتأكد من صدق هذه الفرضية قام الباحث بإجراء اختبار الانحدار الخطي البسيط، وذلك وفقاً للجدول التالي:

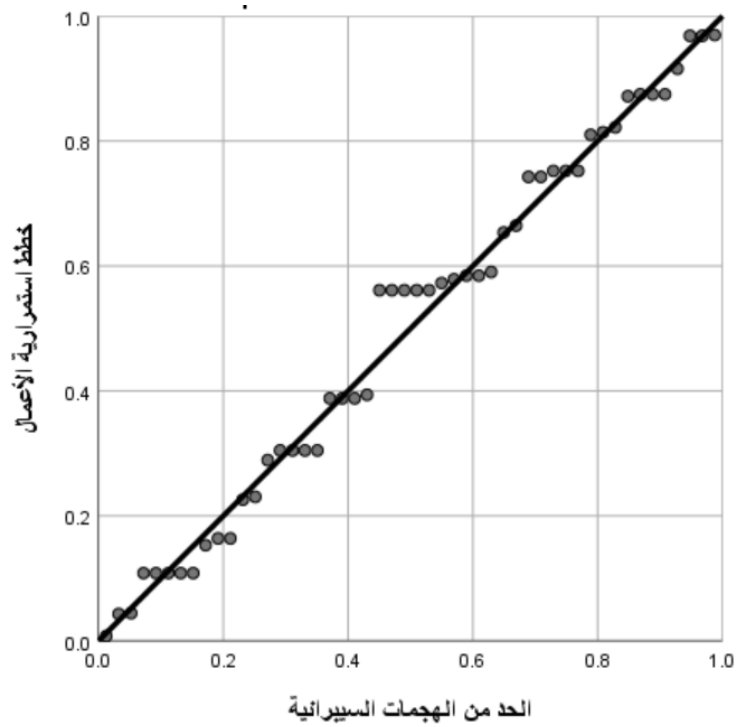
جدول ٩ نتائج تحليل الانحدار الخطي البسيط للفرضية الأولى.

خط	قيمة R	قيمة R ²	قيمة B	قيمة (T)	Sig.
استمرارية					



الأعمال				
للحد من	٠.٧٧٦	٠.٦٠٢	٠.٨٨٩	٨.٥٢٥
الهجمات				
السيبرانية				

يتضح من خلال الجدول السابق أن معامل الانحدار الخطي البسيط للفرضية الثانية يساوي (٠.٧٧٦)، وأن قيمة الارتباط بين أثر خطط استمرارية الأعمال للحد من الهجمات السيبرانية في المملكة العربية السعودية، جاء بمقدار (٨.٥٢٥)، وجاء بمستوى دلالة (٠.٠٠٠) وكان أقل من (٠.٠٥) مما يدل على أنه دال إحصائيًا، لذلك نرفض الفرض الصفري ونقبل بالفرض البديل والذي ينص على أنه: "يوجد أثر ذو دلالة إحصائية لخطط استمرارية الأعمال في المراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية".



شكل ٥ الانحدار الخطي البسيط للفرضية الثانية.

—الفرضية الثالثة:

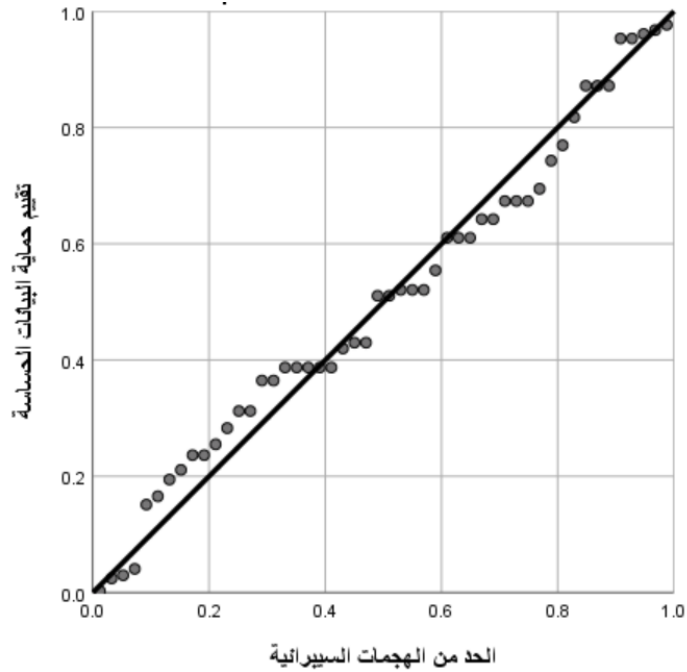
والتي تنص على أنه: "يوجد أثر ذو دلالة إحصائية لتقييم حماية البيانات الحساسة في المراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية"، وللتأكد من صدق هذه الفرضية قام الباحث بإجراء اختبار الانحدار الخطي البسيط، وذلك وفقًا للجدول التالي:



جدول ١٠ نتائج تحليل الانحدار الخطي البسيط للفرضية الثالثة.

خط	قيمة R	قيمة R2	قيمة B	قيمة (T)	Sig.
استمرارية الأعمال					
لحد من الهجمات السيبرانية	٠.٨٤٧	٠.٧١٨	١.٠٢٦	١١.٠٥٥	.000

يتضح من خلال الجدول السابق أن معامل الانحدار الخطي البسيط للفرضية الثالثة يساوي (٠.٨٤٧)، وأن قيمة الارتباط بين أثر تقييم حماية البيانات الحساسة للحد من الهجمات السيبرانية في المملكة العربية السعودية، جاء بمقدار (١١.٠٥٥)، وجاء بمستوى دلالة (٠.٠٠٠) وكان أقل من (٠.٠٥) مما يدل على أنه دال إحصائياً، لذلك نرفض الفرض الصفري ونقبل بالفرض البديل والذي ينص على أنه: "يوجد أثر ذو دلالة إحصائية لتقييم حماية البيانات الحساسة في المراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية".



شكل ٦ الانحدار الخطي البسيط للفرضية الفرعية الثالثة

—الفرضية الرابعة:

والتي تنص على أنه: "توجد فروض ذات دلالة إحصائية لدور إدارة المخاطر واستمرارية أعمالها في المراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية تعزى لمتغير النوع والخبرة والمؤهل العلمي"، وللتحقق من صحة هذه الفرضية قام الباحث بإجراء اختبار T-test واختبار تحليل التباين الأحادي One Way ANOVA، وهو كما بالجدول التالي:

جدول ١١ اختبار لقياس دلالة الفروق لمحاور الاستبيان وفقاً لمتغير

النوع.



المتغير	النوع	العدد	قيمة T	مستوى الدلالة
تقييم إجراءات إدارة المخاطر السيبرانية	ذكر	٣٨	٠.٤٩٣	٠.٥٨٣
	أنثى	١٢		
تقييم خطط استمرارية الأعمال	ذكر	٣٨	٠.١٢٤	٠.٨٩٣
	أنثى	١٢		
تقييم حماية البيانات الحساسة	ذكر	٣٨	١.٠٨٤	٠.٢٢١
	أنثى	١٢		

يتضح من خلال الجدول السابق أن قيمة الاحتمالية لكلاً من محاور الاستبيان وفقاً لمتغير النوع أكبر من مستوى الدلالة (٠.٠٥) بجميع محاور الاستبيان، وهذا يدل على أنها غير دالة إحصائياً، لذلك نقبل الفرض الصفري ونرفض الفرض البديل، وجاءت نتيجة الفرضية بأنه: "توجد فروض ذات دلالة إحصائية لدور إدارة المخاطر واستمرارية أعمالها في المراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية تعزي لمتغير النوع".



جدول ١٢ تحليل التباين الأحادي One Way ANOVA

لمحاور الاستبيان وفقاً لمتغير عدد سنوات الخبرة.

محور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	ف	الدالة الإحصائية
تقييم إجراءات إدارة المخاطر السيبرانية	بين المجموعات	.128	2	.064	.349	.707
	داخل المجموعات	8.643	47	.184		
	المجموع	8.771	49			
	بين المجموعات	.005	2	.003	.014	.986
تقييم خطط استمرارية الأعمال	داخل المجموعات	8.340	47	.177		
	المجموع	8.345	49			
	بين المجموعات	.073	2	.036	.185	.832
	داخل المجموعات	9.252	47	.197		

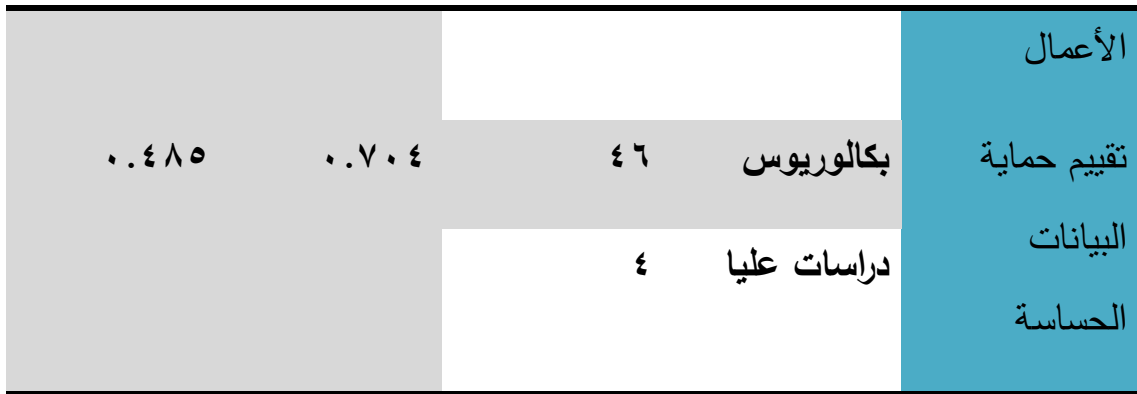


يتضح من خلال الجدول السابق أن قيمة الاحتمالية لكلاً من محاور الاستبيان وفقاً لمتغير عدد سنوات الخبرة أكبر من مستوى الدلالة (٠.٠٥) بجميع محاور الاستبيان، وهذا يدل على أنها غير دالة إحصائياً، لذلك نقبل الفرض الصفري ونرفض الفرض البديل، وجاءت نتيجة الفرضية بأنه: "لا توجد فروق ذات دلالة إحصائية لدور إدارة المخاطر واستمرارية أعمالها في المراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية تعزي لمتغير عدد سنوات الخبرة".

جدول ١٣ اختبار لقياس دلالة الفروق لمحاور الاستبيان وفقاً لمتغير

المؤهل العلمي.

المتغير	المؤهل العلمي	العدد	قيمة T	مستوى الدلالة
تقييم إجراءات إدارة المخاطر السيبرانية	بكالوريوس	٤٦	٠.٦٠٧	٠.٥٤٧
	دراسات عليا	٤		
تقييم خطط استمرارية	بكالوريوس	٤٦	١.٠٨٨	٠.٢٨٢
	دراسات عليا	٤		



يتضح من خلال الجدول السابق أن قيمة الاحتمالية لكلاً من محاور الاستبيان وفقاً لمتغير المؤهل العلمي أكبر من مستوى الدلالة (٠.٠٥) بجميع محاور الاستبيان، وهذا يدل على أنها غير دالة إحصائياً، لذلك نقبل الفرض الصفري ونرفض الفرض البديل، وجاءت نتيجة الفرضية بأنه: "لا توجد فروق ذات دلالة إحصائية لدور إدارة المخاطر واستمرارية أعمالها في المراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية تعزي لمتغير المؤهل العلمي".



النتائج والتوصيات



الخاتمة:

تمثل إدارة المخاطر وإستمرارية الأعمال في مراكز البيانات ركيزة أساسية للحفاظ على أمان واستقرار المنظمات الحكومية والأهلية في المملكة العربية السعودية، وخاصة في مواجهة الهجمات السيبرانية وتحديات فقد البيانات الحساسة، وقد أظهرت الدراسة أن بناء إطار قوي لإدارة المخاطر يستند إلى تحليل شامل للتهديدات السيبرانية وأثرها المحتمل على العمليات، مع أتباع بروتوكولات إستمرارية الأعمال، ويعد من أهم الآليات الوقائية لضمان توفير الحماية القصوى للبيانات والإستمرارية التشغيلية، وهذه الجهود تتماشى مع رؤية المملكة ٢٠٣٠ التي تضع الأمن السيبراني في مقدمة الأولويات، وذلك لما له من تأثير مباشر على حماية معلومات المنظمات ودعم الإقتصاد الرقمي.

أولاً: نتائج الدراسة.

تتمثل نتائج الدراسة الحالية فيما يلي:

- يوجد أثر ذو دلالة إحصائية لتقييم إجراءات إدارة المخاطر السيبرانية في المراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية.



- يوجد أثر ذو دلالة إحصائية لخطط إستمرارية الأعمال في المراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية.

- يوجد أثر ذو دلالة إحصائية لتقييم حماية البيانات الحساسة في المراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية.

- لا توجد فروض ذات دلالة إحصائية لدور إدارة المخاطر واستمرارية أعمالها في المراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية تعزي لمتغير النوع والخبرة والمؤهل العلمي.

- ثانيًا: التوصيات.

أوصت هذه الدراسة بما يلي:

- يجب تطوير إستراتيجيات شاملة لإدارة المخاطر السيبرانية للتركز على تحليل التهديدات، وتقييم احتمالات الاختراق، ووضع خطط استجابة فورية.
- يجب تطبيق برامج تدريبية دورية للموظفين لتعزيز الوعي السيبراني، مع تزويدهم بالأدوات اللازمة للتعامل مع الهجمات الإلكترونية وتجنب الأخطاء البشرية التي تؤدي إلى الإختراقات.



- ضروري تعزيز البنية التحتية للأمن السيبراني من خلال إستخدام أحدث التقنيات والممارسات العالمية للحفاظ على سلامة البيانات، مع اعتماد نظم تشفير متطورة.

- يجب الإلتزام بتطبيق إجراءات النسخ الاحتياطي الدوري للبيانات الحساسة، وتطوير خطط للتعافي من الكوارث تعزز إستمرارية الأعمال وتقليل الآثار الناتجة عن الحوادث السيبرانية.

- يجب التعاون مع الهيئات الوطنية المتخصصة مثل الهيئة الوطنية للأمن السيبراني لإتباع الإرشادات والسياسات التي تضمن توفير معايير عالية من الأمان والإستجابة السريعة للتهديدات.

ثالثاً: مقترحات الدراسة:

تقترح الدراسة الحالية للدراسات الآتية ما يلي:

- تأثير التكنولوجيا الحديثة في تحسين إدارة المخاطر السيبرانية بمراكز البيانات في المملكة العربية السعودية.

- إستراتيجيات إستمرارية الأعمال في مراكز البيانات: دراسة مقارنة بين القطاعات الحكومية والأهلية.

- دور الذكاء الاصطناعي في تعزيز الأمن السيبراني وإستمرارية الأعمال في مراكز البيانات.



- تحليل العلاقة بين وعي الموظفين بالتهديدات السيبرانية وفعالية استمرارية الأعمال في المنظمات السعودية.
- تقييم فعالية سياسات التعافي من الكوارث في مراكز البيانات بالمنظمات السعودية.



قائمة المراجع



أولاً: المراجع العربية:

- ١- البحيصي، عصام و الشريف، ٢٠١١م، حرية، مخاطر نظم المعلومات المحاسبية الالكترونية - دراسة تطبيقية على المصارف العاملة في قطاع غزة، مجلة الجامعة الاسلامية، غزة.
- ٢- برادة، عبد الرزاق والقصير، فتحي، ٢٠٢٤م، الأمن السيبراني ودوره في الحد من الهجمات الإلكترونية، جامعة غليزان، الجزائر.
- ٣- البردان، محمد فوزي أمين و شحاتة، محمد موسى علي، ٢٠٢١م، أثر تفعيل حوكمة تكنولوجيا المعلومات في ظل إستراتيجيات الرقمنة على الحد من مخاطر الهجمات السيبرانية بالبيئة المصرية، كلية التجارة، جامعة مدينة السادات، مصر.
- ٤- حاكمي، نجيب الله، ٢٠١٤م، ادارة المخاطر في المصارف الاسلامية، رسالة ماجستير، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة وهران، الجزائر.
- ٥- حبيب عوفي، ٢٠٢٢م، الفضاء الرقمي تحدي أمني جديد واستراتيجيات الدول في تحقيق الأمن السيبراني العالمي، المجلة الجزائرية للعلوم الانسانية والاجتماعية، الجزائر.



٧- درال، نسيمه ، د-ت، الأمن السيبراني في التجارة الإلكترونية وكيفية

مواجهة مخاطرها (دراسة مقارنة)، أطروحة دكتوراه، جامعة أبو بكر بلقايد

تلمسان الجزائر، كلية الحقوق والعلوم السياسية، الجزائر.

٨- رشوان، عبد الرحمن محمد سليمان وزينب عبدالحفيظ أحمد قاسم،

٢٠٢٢م، أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول

المالي في البنوك، جامعة عمان العربية، المؤتمر العلمي الدولي الأول من

٢٠-٢١ ديسمبر ٢٠٢٢م.

٩- سلام، اسامة عزمي وشقيري، نوري موسى، ٢٠٠٧م، إدارة المخاطر

والتأمين، دار حامد للنشر والتوزيع، الطبعة الأولى، عمان الأردن.

١٠- السمحاني، د-ت، منى عبدالله، متطلبات الأمن السيبراني لأنظمة

المعلومات الادارية بجامعة الملك سعود، كلية التربية، جامعة المنصورة،

مصر.

١١- صوار يوسف، ٢٠٠٨م، محاولة تقدير خطر عدم تسديد القرض

التنقيطي والتقنية العصبية الاصطناعية بالبنوك الجزائرية دراسة حالة بنك)،

رسالة دكتوراه، جامعة تلمسان، الجزائر.

١٢- عبد الجواد، أميرة عبدالعزيز محمد، ٢٠٢٠م، المخاطر السيبرانية وسبل

مواجهتها في القانون العام الدولي ، مجلة الشريعة والقانون، العدد الخامس

والثلاثون.



١٣- عبد الحي، محمد عبد الحميد، ٢٠١٠م، ادارة المخاطر في المصارف

الاسلامية ، دراسة مقارنة، رسالة ماجستير، كلية الاقتصاد جامعة حلب،

سوريا.

١٤- عبد الجواد، محمد وأميرة عبد العظيم، المخاطر السيبرانية وسبل

مواجهتها في القانون العام الدولي، مجلة الشريعة والقانون، العدد الخامس

والثلاثون، ج٣، الجزائر.

١٥- العزاوي، خليل أحمد، ٢٠٠٦م ، إدارة اتخاذ القرار الإداري، دار كنوز

المعرفة للنشر، عمان.

١٦- بن علي بن جدو، ٢٠٢٢م، تحديات الأمن السيبراني مواجهة الجريمة

الالكترونية، المجلة الجزائرية للأمن الإنساني، الجزائر.

١٧- عماد الدين محمد كامل عبد الحميد، ٢٠٢٣م، الهجمات السيبرانية

على البنى التحتية للمدن الذكية،

١٨- العمارات، فارس والحمامصة إبراهيم محمد، ٢٠٢٢م، الأمن السيبراني

- المفهوم وتحديات العصر، دار الخليج للنشر والتوزيع، الاردن.

١٩- فضل عبد الكريم محمد، ٢٠٠٧م، ادارة المخاطر وتحديات المصارف

الاسلامية، اطروحة دكتوراه، جامعة الخرطوم، السودان.



- ٢٠- كلاع، شريفة، ٢٠٢٢م، الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، المجلد ١٥، العدد ١، الجزائر.
- ٢١- لسعري، ٢٠١٩م، انتقال التهديدات من الواقع الى العالم الافتراضي، مجلة جامعة بابل للعلوم الانسانية، العراق.
- ٢٢- المعوفي، حنان محمد وعبد العزيز، محمد رضوان، ٢٠١٧م، إدارة المخاطر في المصارف الاسلامية، مجلة الرسالة، رقم ٢٦٠٠ - ٨٣٩٤، الصادرة سنة ٢٠١٧م.
- ٢٣- الهزاني، نورة بنت ناصر بن عبد الله ، ٢٠٢٣م، ضوابط ومتطلبات تطبيق الأمن السيبراني لحماية البيانات في جامعة الأميرة نورة، مجلة مكتبة الملك فهد الوطنية، العدد الثامن والعشرون، السعودية.

ثانيا: المراجع الاجنبية:

- 24- Babalola, A. O. (2021). Effective Strategies for Cybersecurity and Information Technology Governance for Small Business Leaders: A Quantitative Study (Doctoral dissertation, University of Phoenix).



- 25- Goutam, R. K. Importance of cyber security. International Journal of Computer Applications, (2015).
- 26- Egele, M., Kruegel, C., Kirda, E., Yin, H., & Song, D. Dynamic spyware analysis. . (2007).
- 27- Chou, C., & Peng, H. (2011). Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience. The Internet and Higher Education.
- 28- Conteh, N. Y., & Schmick, P. J. (2021). Cybersecurity Risks Vulnerabilities, and Countermeasures to Prevent Social Engineering Attacks. In Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention (pp. 19-31). IGI Global .



الحق



المكرم الأستاذ / حفظه الله

السلام عليكم ورحمة الله وبركاته. وبعد:

يقوم الباحث بإعداد مشروع بحثي بعنوان " دور إدارة المخاطر واستمرارية أعمالها في مراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية " استكمالاً لمتطلبات الحصول على درجة الماجستير، في تخصص إدارة المخاطر بكلية الإدارة، جامعة ميدأوشن .

وتهدف هذه الدراسة إلى التعرف على دور إدارة المخاطر واستمرارية أعمالها في مراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية، ولتحقيق هذا الغرض تم تصميم أداة للدراسة للتعرف من خلالها على واقع دور إدارة المخاطر واستمرارية أعمالها في مراكز البيانات للحد من الهجمات السيبرانية وفقد البيانات الحساسة في المنظمات الحكومية والأهلية في المملكة العربية السعودية، وتتكون من (١٥) فقرة، وقد صممت الأداة وفقاً لمقياس ليكرت الخماسي على النحو التالي (موافق بشدة، موافق، محايد، غير موافق، غير موافق بشدة) .

ولأهمية رأيك في نتائج البحث آمل التكرم بالإجابة بدقة وموضوعية ووضع علامة في إحدى الخانات الموجودة أمام كل فقره من فقرات الاستبيان ، وذلك بما يتفق مع رأيك ، علماً بأن الغاية من إجراء هذه الدراسة غاية علمية بحثه، حيث سيتم التعامل مع إجابتك وفقاً لقواعد الأمانة والنزاهة العلمية .

شاكر لكم استجابتكم وتعاونكم . والله يحفظكم ويرعاكم ..

الباحث :



القسم الأول: (معلومات عامة)

١ - هل توافق على إجراء البحث

☐ لا

☐ نعم

٢ - الجنس:

☐ أنثى

☐

☐ ذكر

☐

٣ - سنوات الخبرة:

☐ ١٠ سنوات

☐ من ٥ - أقل من ١٠ سنو

☐ أقل من ٥ وات

☐

فأكثر.

٤ - المؤهل العلمي:

☐ دراسات عليا

☐

☐ بكالوريوس

☐



القسم الثاني: الاستبانة ومجالاتها:

أولاً: تقييم إجراءات إدارة المخاطر السيبرانية ؟

م	الفقرات	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
١.	تقوم مؤسستكم بتقييم المخاطر السيبرانية بشكل دوري.					
٢.	يتم تحديد المخاطر السيبرانية الأكثر احتمالاً وخطورة على مؤسستكم .					
٣.	يتم وضع خطط استجابة للطوارئ لمواجهة الهجمات السيبرانية .					
٤.	يتدرب الموظفون بانتظام على كيفية التعامل مع تهديدات الأمن السيبراني .					
٥.	يتم تحديث برامج الحماية والأمن بشكل دوري .					

ثانياً: تقييم خطط استمرارية الأعمال :

م	الفقرات	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
٦.	لدى منظمتك خطة واضحة لاستمرارية الأعمال في حالة حدوث حادث سيبراني .					
٧.	يتم اختبار خطة استمرارية الأعمال بشكل دوري .					



					٨. يتم تحديث خطة استمرارية الأعمال بشكل دوري.
					٩. تخزن منظمتك نسخ احتياطية من البيانات بشكل منتظم .

ثالثاً: تقييم حماية البيانات الحساسة ؟

م	الفقرات	موافق بشدة	موافق	محايد	غير موافق بشدة	غير موافق بشدة
١٠.	تشفر البيانات الحساسة المخزنة في مركز البيانات .					
١١.	تعمل المنظمة على التحقق من هوية المستخدمين قبل منحهم الوصول إلى البيانات الحساسة .					
١٢.	المراقبة للنشاطات المشبوهة في النظام بشكل مستمر.					
١٣.	يتم إجراء تدقيق داخلي وخارجي على إجراءات أمن المعلومات بشكل دوري .					
١٤.	يتم إبلاغ الجهات المختصة في حال حدوث أي اختراق أمني .					