

العنوان باللغة العربية

تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية: استراتيجيات
الحماية والتخفيف

إعداد/

مضاوي محمد المطيري

إشراف/

أسماء أبوعنزه

العام الدراسي:

2024



فهرس المحتويات

5	قائمة الجداول
7	فهرس الأشكال
9	المستخلص Abstract
10	الفصل الأول
11	المقدمة
13	مشكلة الدراسة
15	أهمية الدراسة
20	أهداف الدراسة
21	فروض الدراسة
22	النظرية العلمية المتبعة لإعداد البحث
25	الفصل الثاني
25	الدراسات السابقة
26	مقدمة
28	المتغير التابع والمستقل:
30	الدراسات السابقة
33	الإطار النظري
36	الفصل الثالث
36	منهجية الدراسة
37	مقدمة
39	المنهجية وطرق البحث
41	مجتمع البحث
43	محددات حجم العينة:
46	خطوات جمع البيانات:
49	حدود البحث

51	 الفصل الرابع
51	 نتائج الدراسة
52	 مقدمة
54	 تحليل البيانات
102	 التوصيات
104	 المراجع
105	 المراجع الأجنبية:
107	 الملاحق
110	 الملخص Abstract

قائمة الجداول

- جدول 1: الوصف الاحصائي للبيانات. 57
- جدول 2: الوصف الاحصائي لعمر المشاركين في التجربة. 58
- جدول 3: الوصف الاحصائي لجنس المشاركين. 60
- جدول 4: الوصف الاحصائي لدرجة العلمية للمشاركين. 61
- جدول 5: الوصف الاحصائي لاعتبار الأمن السيبراني أولوية رئيسية في المؤسسات الحكومية. 63
- جدول 6: الوصف الاحصائي لتوفر المؤسسات الحكومية تدريباً كافياً للموظفين حول ممارسات الأمن السيبراني. 65
- جدول 7: الوصف الاحصائي لوجود سياسات واضحة لمواجهة التهديدات السيبرانية في المؤسسات الحكومية. 67
- جدول 8: الوصف الاحصائي لتحديث البرمجيات والتطبيقات بشكل دوري لحماية البيانات الحساسة. 69
- جدول 9: الوصف الاحصائي لتقييمات دورية للمخاطر السيبرانية في المؤسسات الحكومية. 71
- جدول 10: الوصف الاحصائي لاستخدام تقنيات التشفير لحماية البيانات الحساسة في المؤسسات. 73
- جدول 11: الوصف الاحصائي لوجود خطط استجابة واضحة لحالات الطوارئ السيبرانية. 75
- جدول 12: الوصف الاحصائي لتشجيع الموظفين على الإبلاغ عن أي تهديدات تتعلق بالأمن السيبراني. 77
- جدول 13: الوصف الاحصائي لتشجيع المؤسسات الحكومية الابتكار في تقنيات الأمن السيبراني. 78
- جدول 14: الوصف الاحصائي لمستوى الأمن السيبراني في المؤسسات يلبي الاحتياجات الحالية. 80
- جدول 15: الوصف الاحصائي لتقييم المؤسسات أداء مزودي خدمات الأمن السيبراني بشكل دوري. 82
- جدول 16: الوصف الاحصائي لوجود ثقافة مؤسسية تدعم الأمن السيبراني بين جميع الموظفين ... 83
- جدول 17: الوصف الاحصائي لاستخدام أدوات فعالة لرصد التهديدات السيبرانية في المؤسسات ... 85
- جدول 18: الوصف الاحصائي لاعتبار الإجراءات المتخذة لحماية البيانات كافية في المؤسسات الحكومية. 87
- جدول 19: الوصف الاحصائي لمشاركة جميع الموظفين في جهود تعزيز الأمن السيبراني. 89
- جدول 20: الوصف الاحصائي لدعم الميزانية المخصصة للأمن السيبراني في المؤسسات الحكومية. 90

جدول 21: الوصف الاحصائي لوجود آليات لتبادل المعلومات حول التهديدات السيبرانية بين المؤسسات.	92
جدول 24: اختبار كاي اسكوير لدور التدريب الكافي في تقليل المخاطر السيبرانية بالمؤسسات الحكومية بالمملكة العربية السعودية.	95
جدول 25: اختبار كاي اسكوير لدور تحديث البرمجيات في تقليل المخاطر السيبرانية بالمؤسسات الحكومية بالمملكة العربية السعودية.	97
جدول 26: اختبار كاي اسكوير لدور تقنيات التشفير في تقليل المخاطر السيبرانية بالمؤسسات الحكومية بالمملكة العربية السعودية.	99
جدول 22: ملخص انجاز القضية.	100
جدول 23: احصائيات الموثوقية.	101

رسم توضيحي 1: الإطار النظري للدراسة	33
رسم توضيحي 2: التمثيل البياني لعمر المشاركين في التجربة	59
رسم توضيحي 3: التمثيل البياني لجنس المشاركين	60
رسم توضيحي 4: التمثيل البياني لدرجة العلمية للمشاركين	62
رسم توضيحي 5: التمثيل البياني لاعتبار الأمن السيبراني أولوية رئيسية في المؤسسات الحكومية	64
رسم توضيحي 6: التمثيل البياني لتوفر المؤسسات الحكومية تدريباً كافياً للموظفين حول ممارسات الأمن السيبراني	66
رسم توضيحي 7: التمثيل البياني لوجود سياسات واضحة لمواجهة التهديدات السيبرانية في المؤسسات الحكومية	68
رسم توضيحي 8: التمثيل البياني لتحديث البرمجيات والتطبيقات بشكل دوري لحماية البيانات الحساسة	70
رسم توضيحي 9: التمثيل البياني لتقييمات دورية للمخاطر السيبرانية في المؤسسات الحكومية	72
رسم توضيحي 10: التمثيل البياني لاستخدام تقنيات التشفير لحماية البيانات الحساسة في المؤسسات	74
رسم توضيحي 11: التمثيل البياني لوجود خطط استجابة واضحة لحالات الطوارئ السيبرانية	75
رسم توضيحي 12: الوصف الإحصائي لتشجيع الموظفين على الإبلاغ عن أي تهديدات تتعلق بالأمن السيبراني	77
رسم توضيحي 13: التمثيل البياني لتشجيع المؤسسات الحكومية الابتكار في تقنيات الأمن السيبراني	79
رسم توضيحي 14: التمثيل البياني لمستوى الأمن السيبراني في المؤسسات يلبي الاحتياجات الحالية	80
رسم توضيحي 15: التمثيل البياني لتقييم المؤسسات أداء مزودي خدمات الأمن السيبراني بشكل دوري	82
رسم توضيحي 16: التمثيل البياني لوجود ثقافة مؤسسية تدعم الأمن السيبراني بين جميع الموظفين	84
رسم توضيحي 17: التمثيل البياني لاستخدام أدوات فعالة لرصد التهديدات السيبرانية في المؤسسات	86
رسم توضيحي 18: التمثيل البياني لاعتبار الإجراءات المتخذة لحماية البيانات كافية في المؤسسات الحكومية	88

- رسم توضيحي 19: التمثيل البياني لمشاركة جميع الموظفين في جهود تعزيز الأمن السيبراني 89
- رسم توضيحي 20: التمثيل البياني لدعم الميزانية المخصصة للأمن السيبراني في المؤسسات الحكومية 91
- رسم توضيحي 21: التمثيل البياني لوجود آليات لتبادل المعلومات حول التهديدات السيبرانية بين المؤسسات 92
- رسم توضيحي 22: متغيرات الدراسة التابعة والمستقلة 93
- رسم توضيحي 23: المقاييس المتماثلة في تحليل الجداول المتقاطعة لدور التدريب الكافي في تقليل المخاطر السيبرانية بالمؤسسات الحكومية بالمملكة العربية السعودية 95
- رسم توضيحي 24: المقاييس المتماثلة في تحليل الجداول المتقاطعة لدور تحديث البرمجيات في تقليل المخاطر السيبرانية بالمؤسسات الحكومية بالمملكة العربية السعودية 97
- رسم توضيحي 25: المقاييس المتماثلة في تحليل الجداول المتقاطعة لدور تقنيات التشفير في تقليل المخاطر السيبرانية بالمؤسسات الحكومية بالمملكة العربية السعودية 99

المستخلص Abstract

تهدف هذه الدراسة إلى تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية، مع التركيز على استراتيجيات الحماية والتخفيف المتبعة لمواجهة هذه المخاطر. وتأتي هذه الدراسة في ظل التطورات التكنولوجية المتسارعة التي تجعل المؤسسات الحكومية عرضة لتهديدات سيبرانية متزايدة تستهدف البنية التحتية الرقمية. استخدمت الدراسة المنهج الوصفي التحليلي، حيث تم جمع البيانات من خلال استبيانات وزعت على عينة من الموظفين الحكوميين المختصين في مجال الأمن السيبراني، بالإضافة إلى إجراء مقابلات معمقة مع المسؤولين عن أمن المعلومات في بعض المؤسسات. أشارت النتائج إلى أن هناك فجوات في تطبيق بعض استراتيجيات الحماية، خصوصًا في مجال تدريب الموظفين والتحديث المستمر للأنظمة. كما أوضحت النتائج أن المؤسسات الحكومية تعتمد بشكل كبير على الحلول التقنية مثل أنظمة التشفير والجدران النارية، لكنها تحتاج إلى تعزيز التعاون بين الجهات الحكومية وتطوير سياسات أكثر شمولية للتخفيف من المخاطر. توصي الدراسة بضرورة تبني خطط استجابة للحوادث السيبرانية تكون أكثر ديناميكية وتكيفًا مع تطور التهديدات، بالإضافة إلى تطوير برامج توعية مستمرة لتعزيز وعي الموظفين بأهمية الأمن السيبراني.

الكلمات المفتاحية: الأمن السيبراني - المؤسسات الحكومية - المملكة العربية السعودية - استراتيجيات

الحماية، إدارة المخاطر - التخفيف من المخاطر - التهديدات السيبرانية.

الفصل الأول

المقدمة

في ظل التطورات التكنولوجية المتسارعة التي يشهدها العالم اليوم، أصبحت المؤسسات الحكومية أكثر اعتمادًا على الأنظمة الرقمية والتكنولوجيا الحديثة في إدارة عملياتها وتقديم خدماتها. هذا الاعتماد المتزايد على التكنولوجيا يواكبه ارتفاع في مستوى التهديدات السيبرانية التي تستهدف البنية التحتية الحساسة لهذه المؤسسات، مما يجعل الأمن السيبراني قضية محورية تحتاج إلى اهتمام متزايد وإدارة فعالة. في المملكة العربية السعودية، تزايد أهمية هذا الأمر بشكل خاص نظرًا للدور الحيوي الذي تلعبه التكنولوجيا في دعم رؤية 2030، التي تهدف إلى تحقيق تحول رقمي شامل في القطاعات الحكومية والخاصة. ومع هذا التحول، تظهر تحديات جديدة تتعلق بحماية البيانات والمعلومات الحساسة التي تديرها المؤسسات الحكومية، مما يبرز الحاجة إلى استراتيجيات متكاملة لتقييم وإدارة مخاطر الأمن السيبراني (Mishra, 2022).

المؤسسات الحكومية تتعامل يوميًا مع كميات ضخمة من البيانات التي تتضمن معلومات حساسة عن المواطنين، والأمن القومي، والسياسات الحكومية. هذه البيانات ليست فقط قيمة بحد ذاتها، ولكنها أيضًا جزء من بنية تحتية أوسع تضم أنظمة إدارة الهوية، وأنظمة الصحة العامة، والبنية التحتية الحيوية مثل شبكات الطاقة والمياه. تعرض هذه البنية التحتية للخطر يمكن أن يؤدي إلى تداعيات خطيرة على مستوى الدولة ككل، بما في ذلك فقدان الثقة العامة في قدرة الحكومة على حماية مواطنيها وإدارة عملياتها بكفاءة. لذلك، يُعد تقييم المخاطر السيبرانية في هذا السياق أمرًا حيويًا لضمان استمرارية العمل الحكومي وحماية الأمن القومي (Borky, 2018).

تقييم المخاطر السيبرانية هو عملية معقدة تشمل العديد من العناصر، بدءًا من تحديد الأصول القيمة التي تحتاج إلى حماية، وصولًا إلى تحليل التهديدات المحتملة وتحديد نقاط الضعف التي يمكن أن تستغلها هذه التهديدات. في المؤسسات الحكومية، يتطلب هذا التقييم فهمًا دقيقًا للبنية التحتية الرقمية المستخدمة، والتي غالبًا ما تكون معقدة ومتنوعة. تشمل هذه البنية التحتية أنظمة مختلفة تتراوح بين قواعد البيانات الكبيرة إلى تطبيقات الهاتف المحمول التي تُستخدم لتقديم الخدمات العامة. كل مكون من هذه المكونات يمثل نقطة ضعف محتملة يمكن أن تُستغل في حال لم يتم تأمينها بشكل صحيح.

بعد تحديد الأصول ونقاط الضعف، يجب على المؤسسات الحكومية تقدير التأثير المحتمل لأي هجوم سيبراني قد يحدث. هذا يتضمن تحليل السيناريوهات المختلفة التي قد تواجهها المؤسسة، مثل هجمات الحرمان من الخدمة

(DDoS)، أو اختراق البيانات الحساسة، أو هجمات الفدية التي قد تؤدي إلى تعطيل الأنظمة الحيوية. من خلال هذا التحليل، يمكن للمؤسسات تحديد أولوياتها الأمنية والتركيز على حماية الأصول الأكثر أهمية. على سبيل المثال، قد تكون بيانات المواطنين وأنظمة الأمن القومي من بين الأصول التي تتطلب أعلى مستوى من الحماية، وبالتالي يجب توجيه الموارد الأمنية لحمايتها بشكل استباقي (Cremer, 2022).

بمجرد تحديد الأولويات، يأتي دور تطبيق استراتيجيات الحماية التي تهدف إلى تقليل المخاطر إلى أدنى حد ممكن. تعتمد هذه الاستراتيجيات على مزيج من الإجراءات التقنية والتنظيمية التي تعمل معاً لتشكيل دفاعات متعددة الطبقات ضد التهديدات السيبرانية. الإجراءات التقنية تشمل تقنيات مثل التشفير الذي يحمي البيانات أثناء نقلها وتخزينها، وأنظمة مراقبة الشبكات التي تكشف عن الأنشطة المشبوهة في الوقت الفعلي، مما يسمح بالاستجابة السريعة لأي تهديد. بالإضافة إلى ذلك، تأتي الحاجة إلى تطبيق سياسات إدارة الهوية والوصول بصرامة، لضمان أن الأفراد الذين يصلون إلى البيانات الحساسة هم فقط من لديهم التصريح المناسب لذلك، مع استخدام تقنيات متقدمة مثل المصادقة متعددة العوامل لتعزيز الأمان.

فيما يتعلق بالإجراءات التنظيمية، تلعب التوعية والتدريب دوراً محورياً في حماية المؤسسات الحكومية من المخاطر السيبرانية. العامل البشري غالباً ما يكون الحلقة الأضعف في سلسلة الأمن السيبراني، حيث يمكن أن تؤدي الأخطاء البشرية إلى فتح الباب أمام الهجمات. لذلك، يجب على المؤسسات الحكومية الاستثمار في تدريب موظفيها بانتظام على أفضل الممارسات الأمنية، وتعريفهم بالتهديدات الشائعة مثل هجمات التصيد الاحتيالي. هذه الجهود التوعوية يجب أن تكون مستمرة، نظراً لأن طبيعة التهديدات السيبرانية تتطور باستمرار، مما يستدعي تحديث المعلومات والتدابير الأمنية بشكل منتظم (Akter, 2022).

على الرغم من كل التدابير الوقائية، قد تحدث هجمات سيبرانية، ولهذا السبب يجب أن تكون المؤسسات الحكومية مجهزة بخطط استجابة فعالة للحوادث. هذه الخطط تهدف إلى التخفيف من تأثير الهجمات واستعادة العمليات بشكل سريع وفعال. جزء أساسي من هذه الخطط يتضمن تحديد الإجراءات الفورية التي يجب اتخاذها عند اكتشاف تهديد، مثل عزل الأنظمة المتضررة والبدء في عملية التحقيق الجنائي الرقمي لتحديد مصدر الهجوم وكيفية حدوثه. بالإضافة إلى ذلك، يجب أن تتضمن الخطط آليات لاستعادة البيانات والأنظمة المتضررة، بما في ذلك استخدام النسخ الاحتياطية المحمية بشكل جيد لضمان عدم فقدان المعلومات الحيوية.

كما يجب أن تكون خطط الاستجابة ديناميكية، قادرة على التكيف مع التغيرات المستمرة في طبيعة التهديدات. هذا يتطلب من المؤسسات الحكومية إجراء اختبارات دورية لخطط الاستجابة وتحديثها بناءً على نتائج هذه الاختبارات والتغيرات في البيئة الأمنية. كما يجب أن تشمل الخطط تدريبات منتظمة للفرق المتخصصة في الاستجابة للحوادث، لضمان جاهزيتها في مواجهة التهديدات الحقيقية بكفاءة وسرعة.

مع التطور المستمر في تقنيات الهجمات السيبرانية، يجب على المؤسسات الحكومية في المملكة العربية السعودية أن تبقى يقظة ومتقدمة في استخدام أحدث التقنيات الدفاعية. التعاون مع وكالات الأمن السيبراني المحلية والدولية يُعدّ عنصرًا أساسيًا في مواجهة التهديدات المعقدة. هذا التعاون يمكن أن يشمل تبادل المعلومات حول التهديدات السيبرانية والاكتشافات الجديدة، وكذلك الاستفادة من الخبرات العالمية في تطوير استراتيجيات الدفاع السيبراني. علاوة على ذلك، الابتكار في استخدام التكنولوجيا المتقدمة مثل الذكاء الاصطناعي والتعلم الآلي يمكن أن يعزز قدرة المؤسسات على الكشف عن التهديدات والتعامل معها قبل أن تتسبب في أضرار جسيمة (Giannaros, 2023).

يمثل تقييم وإدارة مخاطر الأمن السيبراني في المؤسسات الحكومية عملية مستمرة ومعقدة تتطلب التزامًا طويل الأمد واستثمارًا كبيرًا في الموارد والتكنولوجيا. من خلال تطبيق استراتيجيات الحماية الشاملة وتطوير خطط استجابة فعالة، يمكن للمؤسسات الحكومية تعزيز قدراتها الدفاعية بشكل مستمر وتقليل المخاطر السيبرانية، مما يضمن استمرارية العمليات الحكومية وحماية المعلومات الحساسة من أي تهديدات محتملة. هذه الجهود ليست مجرد استجابة للتحديات الحالية، بل هي أيضًا استثمار في المستقبل، حيث يصبح الأمن السيبراني جزءًا لا يتجزأ من البنية التحتية الوطنية واستقرارها (Dawodu, 2023).

مشكلة الدراسة

• التعقيد والتطور السريع للبنية التحتية الرقمية

تعتمد المؤسسات الحكومية في المملكة العربية السعودية بشكل متزايد على التكنولوجيا الرقمية لإدارة عملياتها وتقديم خدماتها. يشمل هذا الاعتماد العديد من الأنظمة الشبكية المعقدة، والتطبيقات البرمجية المتقدمة، والخدمات السحابية. تتطلب هذه البنية التحتية الرقمية، نظرًا لتعقيدها وتنوعها، إجراءات أمنية متقدمة لحمايتها من التهديدات السيبرانية. المشكلة الأساسية هنا هي القدرة على التقييم الشامل لجميع جوانب هذه البنية التحتية وتحديد نقاط

الضعف المحتملة التي يمكن أن تستغلها الجهات المهاجمة. بالإضافة إلى ذلك، يستدعي هذا الأمر تحديثًا مستمرًا للبنية التحتية الأمنية لتواكب التطورات التكنولوجية السريعة وتضمن حماية مستدامة للبيانات والأنظمة الحيوية.

• التهديدات السيبرانية المعقدة والمتطورة

تتطور التهديدات السيبرانية بوتيرة سريعة وباستخدام تقنيات متقدمة مثل الذكاء الاصطناعي والتعلم الآلي، مما يزيد من تعقيد التحديات التي تواجهها المؤسسات الحكومية. تشمل هذه التهديدات هجمات الحرمان من الخدمة (DDoS)، وهجمات الفدية، واختراق البيانات الحساسة. كل نوع من هذه الهجمات يتطلب استراتيجيات دفاعية مختلفة ومتكاملة لضمان الحماية الشاملة. التحدي الرئيسي هنا يكمن في القدرة على التنبؤ بهذه التهديدات والاستعداد لها بفعالية. تتطلب هذه المهمة تحليلًا دقيقًا لنماذج الهجمات السيبرانية وتطوير حلول مبتكرة تستطيع التعامل مع التهديدات في الوقت الفعلي، مما يضمن حماية الأنظمة الحيوية وتقليل الأضرار المحتملة.

• دور العامل البشري في الأمن السيبراني

يشكل العامل البشري حلقة ضعف رئيسية في سلسلة الأمن السيبراني. غالبًا ما يكون الإهمال أو الافتقار إلى الوعي الأمني السبب الرئيسي وراء نجاح العديد من الهجمات السيبرانية. لذا، يتعين على المؤسسات الحكومية في المملكة العربية السعودية التركيز على تدريب الموظفين وتوعيتهم بأهمية الأمن السيبراني. تشمل هذه البرامج التوعوية تدريب الموظفين على كيفية التعرف على التهديدات الشائعة مثل هجمات التصيد الاحتيالي، والتعامل الصحيح مع البيانات الحساسة. بالإضافة إلى ذلك، يجب أن تشمل هذه البرامج تدريبات دورية وتحديثات مستمرة لضمان مواكبة الموظفين للتطورات الجديدة في مجال التهديدات السيبرانية وكيفية التصدي لها.

• السياسات الأمنية والإجراءات الوقائية

تتطلب حماية البيانات الحساسة في المؤسسات الحكومية تطوير سياسات أمنية قوية وإجراءات حماية متعددة الطبقات. تشمل هذه السياسات استخدام تقنيات التشفير لحماية البيانات أثناء نقلها وتخزينها، وتطبيق أنظمة إدارة الهوية والوصول للتحكم فيمن يمكنه الوصول إلى المعلومات الحساسة. يعتبر وضع خطط استجابة فعالة للحوادث السيبرانية جزءًا أساسيًا من هذه السياسات. يجب أن تشمل هذه الخطط تحديد الإجراءات الفورية التي يجب اتخاذها عند اكتشاف تهديد سيبراني، وتطوير آليات لاستعادة البيانات والأنظمة المتضررة بسرعة لضمان استمرارية العمليات

الحوية. كما يجب أن تكون هذه السياسات ديناميكية وقابلة للتحديث بشكل مستمر لمواكبة التطورات السريعة في مجال التهديدات السيبرانية.

• التعاون والتنسيق بين الجهات المسؤولة

يعتبر التعاون والتنسيق بين مختلف الجهات المسؤولة عن الأمن السيبراني في المؤسسات الحكومية أمراً حيوياً لمواجهة التهديدات السيبرانية بفعالية. يتطلب التصدي للتهديدات السيبرانية تعاوناً وثيقاً بين المؤسسات الحكومية المختلفة، وكذلك التعاون مع القطاع الخاص والوكالات الدولية المتخصصة في الأمن السيبراني. يبرز هنا التحدي في توحيد الجهود وتبادل المعلومات حول التهديدات والتقنيات الدفاعية بين جميع الأطراف المعنية. لذلك، يجب تطوير آليات فعالة للتعاون والتنسيق، بما في ذلك إنشاء مراكز عمليات أمنية مشتركة، وتنظيم تدريبات ومحاكاة دورية للتعامل مع التهديدات السيبرانية، وتبادل المعلومات حول الحوادث والتطورات الجديدة في مجال التهديدات السيبرانية.

• التوازن بين التحول الرقمي والأمن السيبراني

تواجه المؤسسات الحكومية تحدياً كبيراً في تحقيق التوازن بين التحول الرقمي وأمن البنية التحتية الرقمية. التحول الرقمي يعد هدفاً استراتيجياً ضمن رؤية 2030، حيث يسعى إلى تحسين الكفاءة والإنتاجية وتعزيز الابتكار في القطاع الحكومي. ومع ذلك، يجب أن يتم هذا التحول بحذر شديد مع الأخذ في الاعتبار جميع التهديدات الأمنية المحتملة. يتطلب هذا التوازن نهجاً متكاملًا يشمل تقييم المخاطر، وتطبيق استراتيجيات الحماية الفعالة، وضمان استمرارية العمليات حتى في حال حدوث هجمات سيبرانية. يتطلب هذا النهج أيضاً تحديث السياسات والإجراءات الأمنية بشكل دوري لتواكب التغيرات السريعة في البيئة الرقمية وضمان حماية مستدامة للبنية التحتية الرقمية.

أهمية الدراسة

✓ أهمية الدراسة العلمية

تعتبر الدراسة حول تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية ذات أهمية علمية بالغة لأسباب متعددة تتعلق بآثارها على مجالات متعددة تشمل تطوير المعرفة النظرية، وتحسين الممارسات العملية، وتعزيز السياسات والاستراتيجيات الأمنية.

• تعزيز المعرفة النظرية في مجال الأمن السيبراني

تسهم هذه الدراسة بشكل كبير في إثراء المعرفة النظرية المتعلقة بالأمن السيبراني من خلال تقديم تحليل متعمق وشامل للمخاطر التي تواجه المؤسسات الحكومية. تعتمد هذه الدراسة على نماذج وأساليب علمية لتحليل وتقييم المخاطر، مما يضيف إلى الأدبيات العلمية الحالية في هذا المجال. من خلال توسيع قاعدة المعرفة النظرية، تتيح الدراسة للباحثين والأكاديميين فهمًا أفضل للتهديدات السيبرانية وكيفية تقييمها بطرق علمية دقيقة. كما تسهم في تطوير مفاهيم ونظريات جديدة تتعلق بالأمن السيبراني، مما يمكن أن يكون له تأثير كبير على الأبحاث المستقبلية في هذا المجال الحيوي.

• تطوير استراتيجيات الحماية والتخفيف

تلعب هذه الدراسة دورًا حيويًا في تطوير استراتيجيات فعالة للحماية والتخفيف من المخاطر السيبرانية. من خلال التحليل الدقيق لنقاط الضعف والثغرات في الأنظمة الحكومية، يمكن للدراسة تقديم توصيات علمية مبنية على الأدلة حول كيفية تحسين البنية التحتية الأمنية. تساهم هذه التوصيات في تحسين الإجراءات الوقائية وتطوير سياسات أمنية متقدمة تضمن حماية البيانات الحساسة والمعلومات الحيوية. كما تقدم حلولاً مبتكرة لمواجهة التهديدات المتطورة، مما يعزز من قدرة المؤسسات الحكومية على التصدي للهجمات السيبرانية بشكل فعال. تطبيق هذه الاستراتيجيات المبنية على أسس علمية يساهم في تقليل الخسائر المحتملة وتحقيق أمان معلوماتي أعلى.

• تحسين الممارسات العملية والتطبيقية

تعتبر هذه الدراسة أداة قيمة لتحسين الممارسات العملية والتطبيقية في مجال الأمن السيبراني داخل المؤسسات الحكومية. من خلال تقديم أمثلة عملية ودراسات حالة حول كيفية تطبيق استراتيجيات الحماية والتخفيف بشكل فعال، تساعد الدراسة على ترجمة النظريات العلمية إلى ممارسات فعلية يمكن اعتمادها وتنفيذها. تعزز هذه الدراسة القدرة على تقييم فعالية التدابير الأمنية المتبعة وتحديد المجالات التي تحتاج إلى تحسين. بالتالي، تسهم في رفع مستوى الكفاءة والأمان في العمليات الحكومية اليومية، مما ينعكس بشكل إيجابي على جودة الخدمات المقدمة للمواطنين.

• دعم السياسات والاستراتيجيات الوطنية

تلعب هذه الدراسة دورًا محوريًا في دعم السياسات والاستراتيجيات الوطنية المتعلقة بالأمن السيبراني في المملكة العربية السعودية. تقدم الدراسة بيانات وتحليلات دقيقة يمكن استخدامها من قبل صناع القرار لتطوير سياسات أمنية متكاملة وفعالة. كما تسهم في صياغة استراتيجيات وطنية تأخذ في الاعتبار التهديدات السيبرانية المتزايدة وتعمل على

تعزيز القدرة على مواجهتها. هذه الدراسة توفر إطارًا علميًا لصياغة القوانين واللوائح التي تهدف إلى حماية البنية التحتية الحيوية للدولة وضمان استمرارية الأعمال في مواجهة التحديات السيبرانية المتطورة.

• تعزيز التوعية والتعليم في مجال الأمن السيبراني

تساهم الدراسة في تعزيز التوعية والتعليم في مجال الأمن السيبراني من خلال تقديم معلومات قيمة حول المخاطر والإجراءات الوقائية. يمكن استخدام نتائج الدراسة لتطوير برامج تعليمية وتدريبية تهدف إلى رفع مستوى الوعي بين الموظفين الحكوميين وتعزيز فهمهم لأهمية الأمن السيبراني. كما يمكن أن تكون أساسًا لتطوير مناهج دراسية في الجامعات والمؤسسات الأكاديمية، مما يساهم في إعداد جيل جديد من المتخصصين في الأمن السيبراني يتمتعون بالمعرفة والمهارات اللازمة لحماية الأنظمة الرقمية.

• تشجيع البحث والتطوير

تشجع هذه الدراسة على البحث والتطوير المستمر في مجال الأمن السيبراني من خلال تحديد الثغرات والمجالات التي تحتاج إلى مزيد من البحث. تفتح الدراسة آفاقًا جديدة للباحثين لاستكشاف حلول مبتكرة لمشكلات الأمن السيبراني وتطوير تقنيات جديدة لتحسين الحماية والتخفيف. كما تحفز الشركات والمؤسسات التقنية على الاستثمار في تطوير منتجات وخدمات أمنية متقدمة تلبي احتياجات المؤسسات الحكومية وتعزز من قدرتها على التصدي للتهديدات المتزايدة. تعد هذه الدراسة حول تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية ذات أهمية علمية كبيرة، لما تقدمه من إسهامات في تعزيز المعرفة النظرية، وتطوير استراتيجيات الحماية، وتحسين الممارسات العملية، ودعم السياسات الوطنية، وتعزيز التوعية والتعليم، وتشجيع البحث والتطوير. تساهم هذه الدراسة في بناء منظومة أمنية متكاملة وقادرة على مواجهة التحديات السيبرانية المعقدة، مما يضمن حماية الأنظمة الحكومية واستمرارية الخدمات العامة بكفاءة وأمان.

✓ أهمية الدراسة العملية

تتجلى الأهمية العملية لدراسة "تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية: استراتيجيات الحماية والتخفيف" من خلال تأثيرها المباشر والملموس على الواقع العملي والإجراءات التنفيذية في مجال الأمن السيبراني. تغطي هذه الأهمية عدة جوانب حيوية تشمل تحسين مستوى الأمان المعلوماتي، تعزيز الجاهزية والاستجابة للحوادث السيبرانية، تحسين الكفاءة التشغيلية، وتعزيز التعاون بين المؤسسات المختلفة.

• تحسين مستوى الأمان المعلوماتي

تُعتبر هذه الدراسة أداة أساسية لتحسين مستوى الأمان المعلوماتي في المؤسسات الحكومية. من خلال التقييم الشامل للمخاطر السيبرانية وتحديد نقاط الضعف والثغرات في الأنظمة الحالية، يمكن لهذه الدراسة أن تساهم في وضع استراتيجيات حماية فعالة تستند إلى البيانات والتحليلات الدقيقة. يعد تطوير بروتوكولات أمان مخصصة لكل مؤسسة حكومية جزءاً من هذا التحسين، حيث تأخذ هذه البروتوكولات في الاعتبار الاحتياجات الفريدة لكل مؤسسة وتساعد على حماية بياناتها الحيوية من التهديدات المتزايدة. كما أن تنفيذ التوصيات الواردة في الدراسة يمكن أن يقلل من احتمالية حدوث اختراقات أمنية كبيرة، مما يعزز الثقة في البنية التحتية الرقمية للحكومة.

• تعزيز الجاهزية والاستجابة للحوادث السيبرانية

تساهم هذه الدراسة بشكل كبير في تعزيز الجاهزية والاستجابة للحوادث السيبرانية. من خلال تحليل سيناريوهات الهجوم المحتملة ووضع خطط استجابة تفصيلية، تُمكن هذه الدراسة المؤسسات الحكومية من التصرف بسرعة وفعالية عند وقوع هجمات سيبرانية. تتضمن هذه الخطط إجراءات محددة يجب اتباعها في حال اكتشاف تهديد، مما يقلل من الوقت المستغرق للتعافي ويحد من الأضرار المحتملة. بالإضافة إلى ذلك، يمكن استخدام نتائج الدراسة لتطوير تدريبات دورية ومحاكاة لحوادث سيبرانية، مما يساهم في تحسين كفاءة الفرق الأمنية وزيادة وعي الموظفين بكيفية التعامل مع المواقف الطارئة.

• تحسين الكفاءة التشغيلية

يمكن أن تؤدي استراتيجيات الحماية والتخفيف المستمدة من هذه الدراسة إلى تحسين الكفاءة التشغيلية للمؤسسات الحكومية. من خلال تطبيق إجراءات أمان أكثر فعالية وتجنب الانقطاعات الناتجة عن الهجمات السيبرانية، يمكن للمؤسسات الحفاظ على استمرارية الأعمال وتقديم الخدمات العامة بشكل سلس ودون تأخير. بالإضافة إلى ذلك، يؤدي تقليل عدد الحوادث السيبرانية إلى تقليل النفقات المرتبطة بإصلاح الأضرار واستعادة البيانات، مما يتيح توجيه الموارد بشكل أكثر كفاءة نحو المبادرات الأخرى. كما أن الكفاءة التشغيلية المعززة تساهم في تحقيق أهداف رؤية 2030 التي تسعى إلى تحسين جودة الخدمات الحكومية وتعزيز الاعتماد على التكنولوجيا الرقمية.

• تعزيز التعاون بين المؤسسات المختلفة

تلعب هذه الدراسة دورًا مهمًا في تعزيز التعاون بين المؤسسات الحكومية المختلفة وكذلك بين الحكومة والقطاع الخاص. من خلال توفير إطار عمل مشترك لتقييم المخاطر وتطوير استراتيجيات الحماية، يمكن للمؤسسات تبادل المعلومات والخبرات بشكل أكثر فعالية. يعزز هذا التعاون من القدرة على التصدي للتهديدات السيبرانية المشتركة ويخلق بيئة أكثر أمانًا لجميع الأطراف المعنية. كما يمكن أن تسهم هذه الدراسة في إنشاء شبكات تعاون محلية ودولية لمشاركة أفضل الممارسات وأحدث التقنيات في مجال الأمن السيبراني، مما يعزز من مستوى الأمان العام ويقلل من التهديدات التي قد تواجه المؤسسات الحكومية.

• المساهمة في وضع سياسات وتشريعات أكثر فعالية

من الجوانب العملية الهامة لهذه الدراسة هي مساهمتها في وضع سياسات وتشريعات أكثر فعالية في مجال الأمن السيبراني. توفر الدراسة بيانات وتحليلات يمكن استخدامها كأدلة لتطوير أو تحديث السياسات الأمنية. تسهم هذه السياسات في إنشاء بيئة تنظيمية تضمن الامتثال لمعايير الأمن السيبراني وتحفز على تطبيق أفضل الممارسات. كما تساهم في تحديد الأدوار والمسؤوليات بوضوح بين مختلف الجهات المعنية، مما يعزز من الفعالية والانسجام في تنفيذ الإجراءات الأمنية.

• تعزيز الوعي والتدريب المستمر

تلعب الدراسة دورًا حيويًا في تعزيز الوعي بأهمية الأمن السيبراني وتوفير التدريب المستمر للموظفين في المؤسسات الحكومية. من خلال تسليط الضوء على المخاطر المحتملة والإجراءات الوقائية، تساعد الدراسة على رفع مستوى الوعي بين الموظفين بأهمية حماية البيانات والتصرف بشكل صحيح عند مواجهة تهديدات سيبرانية. كما يمكن أن تكون نتائج الدراسة أساسًا لتطوير برامج تدريبية متقدمة تهدف إلى تعزيز مهارات الموظفين وتحديث معارفهم بانتظام لمواكبة التغيرات السريعة في مجال التهديدات السيبرانية.

• دعم الاقتصاد الرقمي

تساهم هذه الدراسة بشكل غير مباشر في دعم الاقتصاد الرقمي بالمملكة العربية السعودية. من خلال تعزيز الأمان المعلوماتي، تزيد الثقة في الخدمات الحكومية الرقمية، مما يشجع على تبني التكنولوجيا الرقمية بشكل أوسع. هذا الدعم يساهم في تحقيق أهداف رؤية 2030 التي تسعى إلى تنويع الاقتصاد وزيادة الاعتماد على الاقتصاد الرقمي. كما أن حماية

البيانات والمعلومات الحكومية بشكل فعال يعزز من جاذبية المملكة للاستثمارات الأجنبية، حيث يشكل الأمن السيبراني عاملاً حاسماً في قرارات المستثمرين.

أهداف الدراسة

تهدف هذه الدراسة إلى معالجة واحدة من أهم القضايا المعاصرة التي تواجه المؤسسات الحكومية في المملكة العربية السعودية، وهي تقييم مخاطر الأمن السيبراني ووضع استراتيجيات فعالة للحماية والتخفيف. يتطلب تحقيق هذا الهدف الرئيسي تحليلاً دقيقاً للمخاطر الحالية، وتحديد الثغرات الأمنية، ووضع خطط شاملة لمواجهتها. يتفرع من هذا الهدف الرئيسي مجموعة من الأهداف الفرعية التي تساعد في تحقيق رؤية متكاملة وشاملة للأمن السيبراني في القطاع الحكومي.

✓ الهدف الرئيسي

- تقييم شامل لمخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية وتطوير استراتيجيات فعالة للحماية والتخفيف من هذه المخاطر.

✓ الأهداف الفرعية

- تحليل الوضع الحالي للأمن السيبراني في المؤسسات الحكومية.
- تهدف هذه الدراسة إلى إجراء تحليل دقيق للوضع الحالي للأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية. يتضمن ذلك تقييم البنية التحتية الأمنية الموجودة، وفحص السياسات والإجراءات المتبعة، وتحديد مستوى الوعي بأهمية الأمن السيبراني بين الموظفين. من خلال هذا التحليل، يمكن تحديد نقاط القوة والضعف في الأنظمة الحالية وتوجيه الجهود نحو المجالات التي تحتاج إلى تحسين.
- تحديد التهديدات السيبرانية الرئيسية التي تواجه المؤسسات الحكومية.
- يركز هذا الهدف الفرعي على تحديد التهديدات السيبرانية الأكثر شيوعاً وخطورة التي تواجه المؤسسات الحكومية. يشمل ذلك تحليل أنواع الهجمات الشائعة مثل الهجمات بالبرمجيات الخبيثة، وهجمات التصيد، وهجمات الفدية، وتحديد مصادر هذه التهديدات سواء كانت من جهات داخلية أو خارجية. يساعد تحديد

هذه التهديدات على توجيه الجهود الأمنية بشكل أكثر فعالية وتركيز الموارد على الحماية من التهديدات الأكثر احتمالاً.

— تقييم تأثير الهجمات السيبرانية على العمليات الحكومية.

يتضمن هذا الهدف الفرعي دراسة تأثير الهجمات السيبرانية على العمليات الحكومية المختلفة، بما في ذلك تأثيرها على تقديم الخدمات العامة، والحفاظ على سرية البيانات، واستمرارية الأعمال. من خلال فهم تأثير هذه الهجمات، يمكن تطوير استراتيجيات للحد من الأضرار والتأكد من استمرارية العمليات الحيوية حتى في حالة وقوع هجوم سيبراني. يتطلب ذلك تحليلاً دقيقاً للحوادث السابقة ودراسة الأضرار التي تسببت فيها هذه الهجمات.

— تطوير إطار عمل شامل لإدارة المخاطر السيبرانية.

تهدف هذا الهدف الفرعي إلى تطوير إطار عمل شامل لإدارة المخاطر السيبرانية يشمل تحديد المخاطر، وتقييمها، وإدارة الاستجابة لها. يتضمن ذلك وضع سياسات وإجراءات موحدة لمواجهة التهديدات السيبرانية، وتحديد الأدوار والمسؤوليات بوضوح، وتطوير خطط استجابة للحوادث. يساعد إطار العمل هذا في تنظيم الجهود وتحسين التنسيق بين مختلف الجهات المعنية بالأمن السيبراني داخل المؤسسات الحكومية.

— تطوير وتنفيذ برامج تدريبية لزيادة الوعي بالأمن السيبراني.

يركز هذا الهدف الفرعي على تطوير برامج تدريبية وتوعوية تستهدف جميع مستويات الموظفين في المؤسسات الحكومية. تهدف هذه البرامج إلى زيادة الوعي بأهمية الأمن السيبراني، وتعزيز فهم الموظفين للتهديدات السيبرانية وكيفية التعامل معها، وتشجيع الممارسات الأمنية الجيدة. يشمل ذلك تنظيم ورش عمل، ودورات تدريبية، وحملات توعية مستمرة لضمان بقاء الموظفين على اطلاع دائم بأحدث التهديدات وأساليب الحماية.

فروض الدراسة

✓ الفرضية الرئيسية

— تطبيق استراتيجيات فعالة لتقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية يساهم بشكل كبير في تحسين مستوى الحماية والتخفيف من المخاطر السيبرانية.

✓ الفرضيات الفرعية

- التهديدات السيبرانية المحددة تؤثر بشكل مباشر على مستوى الأمان السيبراني في المؤسسات الحكومية.
- وجود إطار عمل شامل لإدارة المخاطر السيبرانية يساهم في تحسين فعالية استراتيجيات الحماية والتخفيف.
- تدريب الموظفين وزيادة الوعي بالأمن السيبراني يساهمان في تعزيز الحماية وتقليل المخاطر.
- فعالية استراتيجيات الحماية والتخفيف تتأثر بالتحديات التقنية والتنظيمية التي تواجه المؤسسات.
- التعاون بين المؤسسات الحكومية المختلفة يعزز من فعالية الاستراتيجيات الأمنية ضد المخاطر السيبرانية.

النظرية العلمية المتبعة لإعداد البحث

تعتبر قضايا الأمن السيبراني من القضايا المحورية التي تواجه المؤسسات الحكومية في العصر الرقمي الحالي، حيث تتعرض هذه المؤسسات لهجمات متزايدة تنوع بين الهجمات السيبرانية المتطورة والتهديدات الداخلية. إن هذه التهديدات تمثل تحديًا كبيرًا، خصوصًا في سياق المملكة العربية السعودية، حيث تتسارع جهود التحول الرقمي وتحديث البنية التحتية التكنولوجية. يتناول هذا البحث تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة، مع التركيز على استراتيجيات الحماية والتخفيف. ولذلك، تستند النظرية العلمية المستخدمة في إعداد هذا البحث إلى مجموعة من الأسس والنماذج التي تساعد على فهم المخاطر والتحديات المرتبطة بالأمن السيبراني.

- الإطار النظري

تقوم النظرية العلمية المتبعة في هذا البحث على فهم عميق لمفاهيم الأمن السيبراني وتطبيقها في السياق الحكومي. يتضمن ذلك التعرف على الأنواع المختلفة للتهديدات السيبرانية، مثل الفيروسات والبرمجيات الخبيثة، وكذلك الهجمات الموجهة التي تستهدف البيانات الحساسة. من المهم إدراك أن هذه التهديدات ليست ثابتة، بل تتطور بشكل مستمر، مما يتطلب استراتيجيات استباقية للتصدي لها (Li، 2021).

لتحقيق هذا الهدف، يعتمد البحث على نموذج تقييم المخاطر، الذي يُعتبر أداة أساسية لتحليل المخاطر التي قد تواجهها المؤسسات الحكومية. يتكون هذا النموذج من عدة مراحل، بدءًا من تحديد الأصول الهامة التي تحتاج إلى حماية، وصولًا

إلى تقييم التهديدات التي قد تؤثر عليها. يُعتبر تحديد الأصول المرحلة الأولى، حيث يتعين على المؤسسات الحكومية معرفة البيانات والأنظمة التي تمثل قيمة حيوية، مثل البيانات الشخصية والمالية.

بعد تحديد الأصول، ينتقل البحث إلى تقييم التهديدات المحتملة، والتي تشمل هجمات القرصنة، والتسريب المتعمد للمعلومات، وأيضًا الأخطاء البشرية. هنا يأتي دور تحليل المخاطر، حيث يتم تحديد مستوى التأثير المحتمل لكل تهديد على الأصول، مما يساهم في وضع استراتيجيات فعالة للتخفيف من المخاطر. يتطلب هذا التحليل نهجًا شموليًا يشمل تقييم كل من الاحتمالية والتأثير، حيث تساعد النتائج في توجيه جهود المؤسسات نحو أولويات الحماية (Kaur، 2023).

- استراتيجيات الحماية

تتناول هذه المرحلة استراتيجيات الحماية التي تعتمد عليها المؤسسات الحكومية. إن الأمن السيبراني ليس مجرد استخدام تقنيات معينة، بل هو نظام متكامل يتضمن عدة جوانب. تعتمد المؤسسات الحكومية على استخدام جدران الحماية، وأنظمة كشف التسلل، وتقنيات التشفير لضمان حماية بياناتها. بالإضافة إلى ذلك، يُعتبر التدريب والتوعية من العوامل الأساسية في حماية المعلومات، حيث يلعب العنصر البشري دورًا مهمًا في الحد من المخاطر.

إن تدريب الموظفين على كيفية التعامل مع المعلومات الحساسة وكيفية التعرف على التهديدات السيبرانية يُعد جزءًا أساسيًا من استراتيجية الحماية. إذ يجب على جميع العاملين في المؤسسات الحكومية فهم أهمية الأمن السيبراني وطرق التصدي للهجمات، مما يساهم في بناء ثقافة أمنية قوية داخل المؤسسات (Admass، 2024).

- الإطار التنظيمي والقانوني

يتعلق هذا الجانب بالإطار التنظيمي والقانوني الذي يحكم الأمن السيبراني في المملكة العربية السعودية. تعتبر القوانين والسياسات الحكومية ذات أهمية كبيرة في وضع معايير الحماية وتعزيز الجهود الوطنية في مجال الأمن السيبراني. تعمل الهيئة الوطنية للأمن السيبراني، على سبيل المثال، على وضع السياسات والتوجيهات اللازمة لحماية البيانات والمعلومات الحساسة.

يساهم الإطار التنظيمي في تعزيز التعاون بين مختلف الجهات الحكومية والقطاع الخاص، مما يسهل تبادل المعرفة والخبرات. كما يُساعد هذا التعاون في تطوير استراتيجيات فعالة تساهم في بناء نظام أمني متكامل، يتماشى مع التوجهات العالمية في مجال الأمن السيبراني.

من خلال هذا البحث، يتضح أن تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية يتطلب نهجاً شاملاً يعتمد على تقييم الأصول والتهديدات، بالإضافة إلى وضع استراتيجيات حماية فعالة. إن هذا التقييم لا يقتصر فقط على الجانب التكنولوجي، بل يمتد إلى الجوانب البشرية والتنظيمية. من خلال تقديم إطار عمل مدروس، يسعى البحث إلى تعزيز الأمن السيبراني في المؤسسات الحكومية، مما يساهم في حماية المعلومات الحساسة وضمان استمرارية العمل في بيئة رقمية متطورة (Alhejaili، 2024).

الفصل الثاني

الدراسات السابقة

المقدمة

يمثل الفصل الثاني من هذه الدراسة جزءًا حيويًا يتناول ثلاثة محاور رئيسية تساهم في فهم شامل لتقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية. يتضمن هذا الفصل شرحًا مفصلاً عن متغيرات الدراسة، سواء التابعة منها أو المستقلة، بالإضافة إلى مراجعة الدراسات السابقة ذات الصلة، وأخيرًا الإطار النظري الذي يوجه هذه الدراسة. يهدف هذا الفصل إلى تزويد القارئ بأسس معرفية قوية لفهم المخاطر الحالية والتهديدات السيبرانية، وكذلك استراتيجيات الحماية والتخفيف اللازمة لحماية المؤسسات الحكومية.

سيتم في هذا الفصل تقديم المتغيرات التابعة والمستقلة بشكل مفصل، حيث يُعتبر فهم هذه المتغيرات أمرًا بالغ الأهمية لقياس فعالية الاستراتيجيات المعتمدة في مجال الأمن السيبراني. يشمل ذلك مناقشة المتغير التابع الرئيسي وهو "مخاطر الأمن السيبراني"، الذي يعكس درجة تعرض المؤسسات الحكومية للتهديدات السيبرانية. ومن ناحية أخرى، سيتم تناول المتغيرات المستقلة، مثل "التدريب الكافي" و"تحديث البرمجيات" و"تقنيات التشفير"، وكيف تساهم هذه المتغيرات في تقليل مخاطر الأمن السيبراني. إن دراسة هذه المتغيرات تساعد في تحديد العوامل التي تؤثر بشكل مباشر على مستوى الأمان السيبراني، مما يوفر بيانات قيمة لصانعي القرار في المؤسسات الحكومية.

ستقوم هذه الدراسة أيضًا بمراجعة الأدبيات السابقة المتعلقة بالأمن السيبراني، لا سيما في السياق الحكومي. تعتبر الدراسات السابقة مرجعًا مهمًا لفهم التوجهات الحالية في مجال الأمن السيبراني، وكذلك التحديات التي تواجه المؤسسات الحكومية. من خلال تحليل هذه الدراسات، يمكن استنباط الدروس المستفادة من تجارب الدول الأخرى وكيفية تطبيقها في السياق السعودي. كما ستُعزز هذه المراجعة من قدرة الدراسة الحالية على تقديم رؤى جديدة وابتكارية في التعامل مع المخاطر السيبرانية.

سيتناول الفصل أيضًا الإطار النظري الذي يدعم هذه الدراسة، حيث يمثل الإطار النظري الأساس الفكري الذي يُستند إليه لتوجيه البحث. يتضمن ذلك النظريات والمفاهيم الرئيسية المتعلقة بالأمن السيبراني، والتي تساعد في فهم التفاعلات بين المتغيرات المختلفة. سيساعد هذا الإطار في تقديم تفسير شامل لكيفية تأثير العوامل المستقلة على المتغير التابع، مما يُعزز من مصداقية النتائج والتوصيات التي ستصدر عن البحث.

إن تناول متغيرات الدراسة، والدراسات السابقة، والإطار النظري في هذا الفصل لا يقتصر فقط على تعزيز المعرفة، بل يساهم أيضًا في بناء قاعدة علمية قوية تدعم النتائج والتوصيات. ففهم العوامل المؤثرة في مخاطر الأمن السيبراني يمكن

أن يُساعد المؤسسات الحكومية على اتخاذ قرارات مستنيرة بشأن استراتيجيات الحماية والتخفيف. كما أن مراجعة الأدبيات السابقة تتيح التعرف على الفجوات البحثية التي يمكن أن تُعالج من خلال هذه الدراسة، مما يسهم في تطوير مجال الأمن السيبراني بالمملكة.

يعتبر الإطار النظري أداة ضرورية لتوجيه البحث وضمان اتساقه، حيث يوفر إطارًا لتحديد العلاقات بين المتغيرات ويساعد في تفسير النتائج. من خلال دراسة هذه العناصر بشكل شامل، يُمكن أن تُحقق هذه الدراسة تأثيرًا إيجابيًا على السياسات الأمنية المعتمدة في المؤسسات الحكومية، مما يسهم في تعزيز الأمن السيبراني وحماية المعلومات الحساسة في المملكة العربية السعودية.

المتغير التابع والمستقل:

- المتغير التابع: مخاطر الأمن السيبراني

يُعتبر "مخاطر الأمن السيبراني" هو المتغير التابع الرئيسي في هذه الدراسة، حيث يعكس مدى تعرض المؤسسات الحكومية في المملكة العربية السعودية لمجموعة من التهديدات السيبرانية. يتضمن هذا المتغير مجموعة واسعة من المخاطر، مثل فقدان البيانات، وتسريب المعلومات الحساسة، وهجمات القرصنة، والفيروسات، والبرمجيات الخبيثة. كل هذه المخاطر تمثل تهديدًا لسلامة المعلومات وأمن البيانات في المؤسسات الحكومية، مما قد يؤدي إلى آثار سلبية كبيرة، مثل فقدان الثقة العامة، والتعرض للعقوبات القانونية، والإضرار بالسمعة المؤسسية.

تُقاس مخاطر الأمن السيبراني بناءً على عدة عوامل، تشمل التهديدات المحتملة، ونقاط الضعف في الأنظمة، والتأثيرات المحتملة لهذه التهديدات على الأصول الحيوية. كما يُعتمد على تحليل شامل لفهم كيف يمكن أن تؤثر المخاطر السيبرانية على العمليات الحكومية الأساسية وبيانات المواطنين. من خلال دراسة هذا المتغير، يمكننا استنتاج مدى فعالية التدابير الأمنية المعتمدة في المؤسسات الحكومية وقدرتها على التصدي لهذه المخاطر، وبالتالي تحديد مدى الحاجة إلى تحسين الاستراتيجيات الحالية.

- المتغيرات المستقلة

1. التدريب الكافي

يعتبر "التدريب الكافي" أحد المتغيرات المستقلة الرئيسية في هذه الدراسة. يشير إلى البرامج التدريبية التي يتم تقديمها للموظفين في المؤسسات الحكومية لتعزيز وعيهم بمخاطر الأمن السيبراني وكيفية التعامل معها. يشمل هذا التدريب موضوعات متنوعة، مثل كيفية التعرف على الهجمات السيبرانية، وممارسات الأمان الأساسية، وأهمية حماية المعلومات الحساسة.

إن التدريب الجيد يمكن أن يسهم بشكل كبير في تقليل مخاطر الأمن السيبراني، حيث يُمكن الموظفين من اتخاذ قرارات مدروسة في مواقف الطوارئ. من خلال تحسين مهاراتهم وكفاءاتهم، يصبح الموظفون أكثر قدرة على التعرف على التهديدات المحتملة والتفاعل معها بفاعلية. على سبيل المثال، قد يتعلم الموظفون كيفية التعرف على رسائل البريد

الإلكتروني الاحتياالية أو الروابط المشبوهة، مما يساعد في الحد من احتمالية وقوع هجمات تصيد. لذلك، يعد التدريب الكافي عاملاً حاسماً في تعزيز الثقافة الأمنية داخل المؤسسات الحكومية، وبالتالي تقليل مخاطر الأمن السيبراني.

2. تحديث البرمجيات

يمثل "تحديث البرمجيات" متغيراً مستقلاً آخر له تأثير كبير على مستوى مخاطر الأمن السيبراني. يتعلق هذا المتغير بالتحديثات الدورية التي تُجرى على البرمجيات والأنظمة المستخدمة في المؤسسات الحكومية. تُعتبر هذه التحديثات ضرورية للغاية، حيث إنها تُعزز من حماية الأنظمة ضد الثغرات الأمنية المعروفة.

تعمل التحديثات على تصحيح الأخطاء البرمجية والثغرات التي يمكن أن يستغلها المهاجمون للدخول إلى الأنظمة. من خلال الحفاظ على البرمجيات محدثة، تتمكن المؤسسات من تقليل احتمالية تعرضها لهجمات سيبرانية ناجحة. كما أن التحديثات توفر ميزات جديدة وتحسينات للأداء، مما يساهم في تعزيز كفاءة الأنظمة. لذا، يعد تحديث البرمجيات جزءاً أساسياً من استراتيجية الأمن السيبراني الفعالة، ويساعد في تقليل المخاطر التي تواجه المؤسسات الحكومية.

3. تقنيات التشفير

"تقنيات التشفير" هي المتغير المستقل الثالث في هذه الدراسة. تشير إلى الأساليب المستخدمة لحماية البيانات والمعلومات الحساسة من الوصول غير المصرح به. يُعتبر التشفير من أهم الأدوات المستخدمة في الأمن السيبراني، حيث يعمل على تحويل البيانات إلى شكل غير قابل للقراءة إلا من قبل الأشخاص المصرح لهم فقط.

تساعد تقنيات التشفير في حماية البيانات أثناء نقلها أو تخزينها، مما يقلل من مخاطر التعرض للسرقة أو التسريب. على سبيل المثال، عند استخدام التشفير في الاتصالات الحكومية، يمكن ضمان سرية المعلومات المتبادلة، مما يعزز الثقة بين الجهات الحكومية والمواطنين. وبالتالي، يعد استخدام تقنيات التشفير جزءاً أساسياً من استراتيجية الأمن السيبراني، حيث يساهم في تقليل مخاطر الأمن السيبراني من خلال ضمان سلامة البيانات.

تستند هذه الدراسة إلى مجموعة من المتغيرات التي تلعب دوراً حاسماً في تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية. من خلال فهم كيفية تأثير التدريب الكافي، وتحديث البرمجيات، وتقنيات التشفير على مستوى المخاطر، يمكن وضع استراتيجيات فعالة لتحسين الأمن السيبراني وحماية المعلومات الحساسة. إن التركيز

على هذه المتغيرات يسهم في تعزيز الثقافة الأمنية داخل المؤسسات الحكومية، مما يعكس أهمية الاستعداد والاستجابة للتهديدات السيبرانية المتزايدة.

الدراسات السابقة

تعاني العديد من المنظمات في جميع أنحاء العالم من خسائر فادحة بسبب المخاطر غير المتوقعة التي يمكن أن يكون لها تأثير عميق على بقائها. تقدم هذه الورقة إطارًا أمنيًا جديدًا لتلبية الاحتياجات الأمنية للمنظمات السعودية. هناك أربع مراحل في إطار الأمن: تقييم المخاطر وإدارتها، والاستخبارات الأمنية والتحليلات، وسياسات وإجراءات الأمن، ومراقبة الأمن. تم توفير حل أمني شامل من خلال الجمع بين أطر الأمن المشتركة، على سبيل المثال: ISO / IEC 27001: 2013، وإطار الأمن السيبراني NIST، وCOBIT. تم تصميم الإطار المتطور لمساعدة المنظمات السعودية على تحديد المخاطر وتقييمها والسيطرة عليها والاستجابة للأحداث غير المتوقعة في الوقت المناسب وبطريقة فعالة. ومن المتوقع أن يساعد المنظمات على تطوير وتنفيذ تدابير أمنية فعالة لحماية أصولها وعملياتها الحيوية من التهديدات الأمنية. الإطار المقترح شامل ويمكن أن يغطي متطلبات معظم المنظمات (Alshammari, 2023).

حققت المملكة العربية السعودية إنجازات كبيرة في مجال الأمن السيبراني. فقد حافظت المملكة العربية السعودية على آليات تنظيمية قوية لمنع وتبعية ومعاينة المخالفين لحماية مصالح المستخدمين الأفراد والمنظمات من التهديدات عبر الإنترنت المتمثلة في سرقة البيانات. كما يعزز الاستخدام الواسع النطاق لتكنولوجيا المعلومات وخدمات تمكين تكنولوجيا المعلومات تدابير الأمن. وتعتبر التهديدات السيبرانية المتطورة باستمرار موضوعًا يثير الكثير من المناقشات. وفي هذا الصدد، تسلط هذه المقالة الضوء على منظور واسع النطاق حول كيفية تطور الجرائم الإلكترونية في المملكة العربية السعودية في الوقت الحاضر، كما تلقي نظرة على بعض أهم الهجمات التي وقعت في المنطقة. وتهدف الأطر التشريعية والتدابير الحالية في المملكة العربية السعودية إلى ردع النشاط الإجرامي عبر الإنترنت. وقد تم ابتكار نماذج كفاءة مختلفة لمعالجة الكفاءات اللازمة لمكافحة الجرائم الإلكترونية في هذا السياق. ويمكن للمتخصصين في البحث في هذا المجال الاستفادة بشكل أكبر من خلال تطوير مستوى كفاءة رئيسي لتحقيق أقصى قدر من الأمن. لمعالجة هذا السؤال البحثي، يستخدم التقييم الحالي مختبر تجربة وتقييم صنع القرار الضبابي (Fuzzy-DMTAE)، وعملية التسلسل الهرمي التحليلي الضبابي (F.AHP)، ومنهجية Fuzzy TOPSIS لتحقيق تطوير الكفاءة على مستوى القطاعات

في سياسة الأمن السيبراني. كما تمت مناقشة أوجه التشابه والاختلاف بين الطرق الثلاث. حدد تحليل الأمن السيبراني هذا أن المركز الوطني للأمن السيبراني حصل على أعلى أولوية. وتختتم الدراسة بدراسة التحديات التي لا تزال بحاجة إلى الفحص والحل في إحداث آليات أمان عبر الإنترنت أكثر مصداقية وفعالية لتقديم اقتصاد أكثر تمكينًا مدفوعًا بخدمات تكنولوجيا المعلومات للمملكة العربية السعودية. علاوة على ذلك، يحتاج المتخصصون في الأمن السيبراني وصناع السياسات إلى جمع جهودهم لحماية الأصول الرقمية للبلاد في عصر الحرب السيبرانية العلنية والسرية (Alhakami, 2024).

اقترحت حكومة المملكة العربية السعودية أطر عمل مختلفة مثل إطار تنظيم الأمن السيبراني لهيئة الاتصالات وتقنية المعلومات وضوابط الأمن السيبراني الأساسية للهيئة الوطنية للأمن السيبراني لضمان أمن البيانات والبنية الأساسية في جميع الأنظمة القائمة على تكنولوجيا المعلومات. ومع ذلك، تفتقر هذه الأطر إلى آلية عملية منشورة تقيم باستمرار مستوى أمن المنظمات، وخاصة في أنظمة مؤسسات التعليم العالي. تقترح هذه الورقة إطار عمل لتقييم الأمن السيبراني لمؤسسات التعليم العالي في المملكة العربية السعودية. SCMAF هو إطار عمل شامل ومخصص لتقييم نضج الأمن للمؤسسات السعودية يتماشى مع معايير الأمن المحلية والدولية. يمكن استخدام الإطار كطريقة تقييم ذاتي لتحديد مستوى الأمان وتبسيط الضوء على نقاط الضعف وخطط التخفيف التي يجب تنفيذها. SCMAF هو نموذج رسم وترميز لجميع اللوائح التي يجب على المؤسسات السعودية الامتثال لها. يستخدم الإطار مستويات مختلفة من النضج يمكن من خلالها قياس أداء الأمن لكل مؤسسة. تم تنفيذ SCMAF كأداة تقييم خفيفة الوزن يمكن توفيرها عبر الإنترنت من خلال خدمة تعتمد على الويب أو دون اتصال بالإنترنت من خلال تنزيل الأداة لضمان خصوصية بيانات المنظمات. يمكن للمنظمات التي تطبق هذا الإطار تقييم مستوى أمان أنظمتها وإجراء تحليل للفجوات وإنشاء خطة للتخفيف. يتم توصيل نتائج التقييم إلى المنظمة باستخدام مخططات النتائج المرئية لكل متطلب أمني لكل مستوى مرفقة بتقرير تقييم (Almomani, 2021).

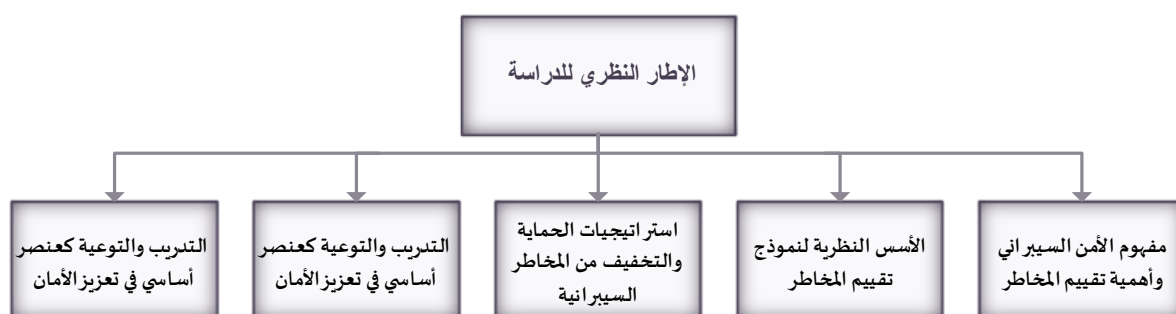
لقد تصاعد تطور أنظمة المعلومات بشكل كبير خلال العقد الماضي حيث كشفت الأبحاث عن مفاهيم جديدة. إن التوجه العام لتوفير حلول للمشاكل المعقدة لا يزال يلهم الإبداع والتقدم الجديد. يبرز الأمن السيبراني كعامل حاسم للنظر فيه ضمن النموذج الناتج حيث أصبحت أنظمة المعلومات متكاملة بشكل كبير. تقدم هذه الورقة تحليلاً متعمقاً للأمن السيبراني في سياق أنظمة المعلومات. تدرس الورقة بعض الجوانب الأكثر أهمية للأمن السيبراني من منظور مشروع

الحكومة الإلكترونية في المملكة العربية السعودية. يتم اقتراح نظام شامل ضمن إطار البحث لدمج المبادئ التوجيهية العلمية المختلفة. يعتمد التوجه العام لهذا البحث على الطموح لتصميم وتنفيذ إطار معقد وقوي يمكن لنظام الحكومة الإلكترونية من خلاله أن يزدهر في سياق المملكة العربية السعودية. يتم أيضًا النظر في البيئة المادية التي سيعمل فيها المشروع، مع التركيز على الأمن. يعكس تقييم بيئة الأمن السيبراني في المملكة العربية السعودية التقدم الكبير الذي حدث في مجالات أنظمة المعلومات خلال السنوات القليلة الماضية (Alrubaiq, 2021).

إن المملكة العربية السعودية لديها هدف يتمثل في ضمان وجود مدينتين على الأقل ضمن أفضل 100 مدينة ذكية في المستقبل. ومع ذلك، فإن زيادة الاتصال ودمج الحلول الذكية في المدن لا يزال يثير المخاوف بشأن الأمن السيبراني مع التهديدات التي تنشأ يوميًا بما في ذلك رفض الخدمات والتصيد الاحتيالي كأحد أهم التهديدات. وبالتالي، تحتاج المملكة العربية السعودية إلى إطار عمل لسياسة الأمن السيبراني يضمن الحماية الفعالة لجميع أصحاب المصلحة في المدينة الذكية من هذه التهديدات السيبرانية. يعد قبول المستخدم هو الأهم في أي تقنية جديدة، بما في ذلك المدن الذكية. وبسبب التهديدات السيبرانية المستمرة وفي غياب سياسات سيبرانية فعّالة، فإن مجتمع المستخدم النهائي السعودي ليس حريصًا على قبول التقنيات الأحدث حيث يتطلب تفاعله مع الوسائط عبر الإنترنت. يتيح انتشار المدن الذكية عالميًا الفرصة لتحليل ومقارنة الجهود المبذولة في المملكة العربية السعودية مع دول أخرى مثل الولايات المتحدة الأمريكية والهند وسنغافورة التي تعد نموذج المدينة الذكية الرائد في العالم حاليًا. تتناول هذه المراجعة أوجه التشابه والاختلاف بين إطار سياسة الأمن السيبراني في المملكة العربية السعودية مع هذه الدول الثلاث. ستتناول المراجعة بعض الخصائص والأساليب المحددة للأمن السيبراني في المدن الذكية في الولايات المتحدة الأمريكية والهند وسنغافورة. وبعد مراجعة الإطار الحالي في المملكة العربية السعودية، ستقدم هذه الورقة اقتراحات مثل تحديث تشريعات الجرائم الإلكترونية في المملكة العربية السعودية كما هو الحال في الولايات المتحدة أو صياغة خطة رئيسية للأمن السيبراني كما هو الحال في سنغافورة والتي من شأنها تحسين إطار المملكة العربية السعودية من خلال إنشاء أفضل نموذج إداري للأمن السيبراني في مدنها الذكية (Alhalafi, 2021).

الإطار النظري

في عصر التكنولوجيا الرقمية، أصبحت المخاطر السيبرانية واحدة من أبرز التهديدات التي تواجه المؤسسات الحكومية في المملكة العربية السعودية. يشكل تقييم مخاطر الأمن السيبراني في هذه المؤسسات موضوعاً بالغ الأهمية، إذ يلعب دوراً حيوياً في ضمان استمرارية العمل وحماية المعلومات الحساسة والأنظمة الحيوية. من خلال فهم المنطلقات النظرية التي تقوم عليها دراسة هذا الموضوع، يمكن تسليط الضوء على الأسس التي تعتمد عليها استراتيجيات الحماية والتخفيف، مما يساهم في تعزيز الأمن السيبراني وحماية البنية التحتية المعلوماتية.



رسم توضيحي 1: الإطار النظري للدراسة

• مفهوم الأمن السيبراني وأهمية تقييم المخاطر

الأمن السيبراني يشير إلى مجموعة التدابير والتقنيات والسياسات التي تهدف إلى حماية الأنظمة الحاسوبية والشبكات والمعلومات من التهديدات والاختراقات السيبرانية. يشمل ذلك تأمين البيانات من السرقة أو التعديل غير المصرح به، وضمان استمرارية التشغيل، وحماية الخصوصية. في المؤسسات الحكومية، يعتبر الأمن السيبراني أكثر أهمية نظراً لحساسية المعلومات التي تديرها والتي قد تشمل بيانات شخصية، معلومات حساسة تتعلق بالأمن الوطني، والبيانات المالية.

تقييم مخاطر الأمن السيبراني هو عملية منهجية تهدف إلى تحديد وتحليل المخاطر التي قد تؤثر على الأمان السيبراني للمؤسسات. يتضمن ذلك دراسة التهديدات المحتملة، وتحديد نقاط الضعف في الأنظمة، وتقدير الأثر المحتمل لهذه التهديدات. يُعد هذا التقييم خطوة أساسية في تطوير استراتيجيات فعالة للحماية والتخفيف من المخاطر، حيث يساعد في تحديد أولويات الأمان وتركيز الموارد على التهديدات الأكثر خطورة (Pryimenko, 2024).

• الأسس النظرية لنموذج تقييم المخاطر

نموذج تقييم المخاطر هو إطار عمل يساعد في تحديد وتقدير وتحليل المخاطر السيبرانية. يتألف النموذج من عدة خطوات رئيسية تبدأ بتحديد الأصول التي تحتاج إلى حماية. هذه الأصول قد تشمل البيانات الحساسة، الأنظمة الحيوية، والبنية التحتية التقنية. يتطلب تحديد الأصول فهماً عميقاً لمحتويات المعلومات وقيمتها بالنسبة للمؤسسة. بعد ذلك، يتم تحديد التهديدات المحتملة التي قد تستهدف هذه الأصول. يشمل ذلك التعرف على الهجمات الإلكترونية الشائعة مثل البرمجيات الخبيثة، وهجمات الفدية، وهجمات التصيد.

الخطوة التالية هي تقييم الثغرات في الأنظمة والإجراءات الأمنية. هذا يتضمن فحص نقاط الضعف المحتملة التي يمكن أن يستغلها المهاجمون، مثل ضعف الأمان في البرمجيات، أو نقص في تحديث الأنظمة. بعد تحديد الثغرات، يتم تقدير الأثر المحتمل لكل تهديد على المؤسسة، بما في ذلك التأثير على العمليات التشغيلية، وسرية المعلومات، وسمعة المؤسسة. أخيراً، يتم دمج نتائج تحليل التهديدات والثغرات والأثر لتحديد مستوى المخاطر وإيجاد استراتيجيات لتخفيف هذه المخاطر (Kure, 2021).

• استراتيجيات الحماية والتخفيف من المخاطر السيبرانية

تستند استراتيجيات الحماية والتخفيف إلى مجموعة من المبادئ والأسس النظرية التي تهدف إلى تعزيز الأمان السيبراني. تعتمد هذه الاستراتيجيات على مفهوم الدفاع المتعدد الطبقات، الذي يتضمن استخدام مجموعة من التدابير الأمنية المختلفة لتوفير حماية شاملة. يشمل ذلك استخدام الجدران النارية، وبرامج مكافحة الفيروسات، وأنظمة الكشف عن التسلل، وأنظمة التحكم بالوصول. الفكرة هي أن كل طبقة من هذه الطبقات تعزز الأمان وتضيف حماية إضافية ضد التهديدات (Obi, 2024).

استراتيجية أخرى هي إدارة الثغرات، التي تركز على التعرف على نقاط الضعف في الأنظمة والعمل على إصلاحها. يشمل ذلك تحديث البرمجيات بانتظام، وتطبيق التصحيحات الأمنية، وإجراء اختبارات اختراق دورية لتحديد الثغرات قبل أن يستغلها المهاجمون. بالإضافة إلى ذلك، تكتسب استراتيجيات الاستجابة للحوادث أهمية كبيرة، حيث تشمل إنشاء خطط للاستجابة السريعة والفعالة للحوادث الأمنية، وتحديد الفرق المسؤولة عن التعامل مع هذه الحوادث، وتحليل أسبابها، وتطوير استراتيجيات لاستعادة الأنظمة والبيانات.

• التدريب والتوعية كعنصر أساسي في تعزيز الأمان

أحد الأسس النظرية الهامة في استراتيجيات الحماية والتخفيف هو أهمية التدريب والتوعية. برامج التدريب والتوعية تلعب دوراً حاسماً في زيادة وعي الموظفين بالمخاطر السيبرانية وكيفية التعامل معها. إن تحسين الوعي حول الأمن السيبراني وتعليم الموظفين كيفية التعرف على التهديدات وكيفية التعامل معها يمكن أن يساهم بشكل كبير في تقليل الأخطاء البشرية التي قد تؤدي إلى خروقات أمنية. تتضمن هذه البرامج التدريبية دورات تعليمية، وورش عمل، وحملات توعية منتظمة (Olabode, 2023).

• التعاون والتنسيق بين المؤسسات

استراتيجية التعاون والتنسيق تعد من العوامل الهامة في تعزيز الأمن السيبراني. يشمل التعاون بين المؤسسات الحكومية تبادل المعلومات حول التهديدات والحوادث السيبرانية، وتطوير استراتيجيات حماية مشتركة. يعزز التعاون المشترك من قدرة المؤسسات على التصدي للتهديدات بشكل جماعي، ويحقق حماية أفضل. يشمل هذا التعاون تطوير قنوات للتواصل، وتنسيق الجهود لمواجهة التهديدات المشتركة، وإنشاء فرق عمل مشتركة لتحليل الحوادث وتطوير حلول فعالة (Lostri, 2022).

تشكل المنطلقات النظرية أساساً لفهم الأبعاد المختلفة للأمن السيبراني وتقييم المخاطر في المؤسسات الحكومية. من خلال دراسة مفاهيم الأمن السيبراني، ونموذج تقييم المخاطر، واستراتيجيات الحماية والتخفيف، والتدريب والتوعية، والتعاون بين المؤسسات، يمكن تطوير استراتيجيات فعالة لتعزيز الأمن السيبراني وحماية الأنظمة والبيانات في المؤسسات الحكومية بالمملكة العربية السعودية. هذه المنطلقات توفر إطاراً متكاملًا يساعد في فهم التحديات وتقديم حلول مبتكرة لضمان أمان المعلومات واستمرارية العمل في ظل التهديدات المتزايدة.

الفصل الثالث

منهجية الدراسة

المقدمة

يمثل الفصل الثالث من هذه الدراسة محورًا أساسيًا يتعلق بالمنهجية وطرق البحث المستخدمة لتقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية. يتناول هذا الفصل شرحًا شاملاً للمنهجية البحثية المتبعة، وتحديد مجتمع البحث، وحدود البحث، بالإضافة إلى محددات حجم العينة، وخطوات جمع البيانات. يهدف هذا الفصل إلى تقديم إطار واضح وعلمي يوضح كيفية إجراء البحث وجمع المعلومات اللازمة لتحقيق الأهداف المرجوة.

ستبدأ الدراسة بتوضيح المنهجية البحثية التي تم اختيارها. يُعتبر اختيار المنهجية المناسبة أحد العناصر الحيوية في أي بحث علمي، حيث يؤثر بشكل مباشر على نوعية النتائج وصحتها. في هذه الدراسة، سيتم اعتماد منهجية وصفية تحليلية، والتي تُعد مناسبة لفهم الظواهر المعقدة مثل مخاطر الأمن السيبراني. ستتضمن المنهجية مجموعة من الأدوات والطرق، مثل الاستبيانات والمقابلات، لجمع المعلومات من المشاركين. يتيح هذا الأسلوب للباحثين استكشاف الآراء والتجارب المباشرة من المتخصصين في مجال الأمن السيبراني، مما يُعزز من فهم المخاطر الحالية.

سيتناول هذا الفصل أيضًا تحديد مجتمع البحث، وهو مجموعة المؤسسات الحكومية التي سيتم دراستها. يُعتبر تحديد المجتمع البحثي خطوة مهمة، حيث يُعكس التنوع والاختلاف في المؤسسات الحكومية بالمملكة. سيتم اختيار مجموعة متنوعة من المؤسسات، مثل الوزارات والهيئات الحكومية، لتقديم صورة شاملة عن التحديات التي تواجهها. من خلال دراسة مجتمع البحث، يمكن للباحثين فهم مدى شيوع المخاطر السيبرانية واستراتيجيات الحماية المعتمدة في مختلف المؤسسات.

يتعين تحديد حدود البحث لتجنب توسيع نطاق الدراسة بشكل يؤثر على دقتها. ستتناول هذه الفقرة القيود الجغرافية، مثل التركيز على المؤسسات الحكومية داخل المملكة العربية السعودية، بالإضافة إلى القيود الزمنية، مثل فترة جمع البيانات. تساعد حدود البحث في تحديد نطاق الدراسة، مما يساهم في تعزيز دقة النتائج وتوجيه التوصيات.

ستركز هذه حدود البحث على محددات حجم العينة المستخدمة في الدراسة. يُعتبر اختيار حجم العينة أمرًا حيويًا، حيث يؤثر بشكل مباشر على صلاحية النتائج. سيتم توضيح العوامل التي تؤخذ في الاعتبار عند تحديد حجم العينة، مثل توافر الموارد، والزمن، والجدول الزمني لجمع البيانات. كما سيتم استخدام أساليب إحصائية لتحديد حجم العينة الأمثل، مما يعكس التنوع داخل مجتمع البحث ويُعزز من موثوقية النتائج.

سيتناول الفصل أيضًا خطوات جمع البيانات، والتي تشمل إعداد الاستبيانات، وإجراء المقابلات، وتحديد الطرق المناسبة لجمع المعلومات. سيتم تصميم استبيانات تهدف إلى جمع معلومات دقيقة حول مخاطر الأمن السيبراني، ومستوى الوعي، واستراتيجيات الحماية المستخدمة. ستتضمن هذه الخطوات توضيح كيفية تحليل البيانات التي سيتم جمعها وكيفية استخدامها لاستخلاص النتائج والتوصيات.

إن تناول المنهجية وطرق البحث في هذا الفصل يعد أمرًا بالغ الأهمية، حيث يمثل الأساس الذي يُبنى عليه البحث بأكمله. يُعتبر اختيار منهجية البحث المناسبة أمرًا حيويًا لتحديد كيفية الحصول على بيانات دقيقة وموثوقة. كما أن تحديد مجتمع البحث وحدوده يساهم في التركيز على جوانب معينة من الأمن السيبراني داخل المؤسسات الحكومية، مما يتيح فهمًا أعمق للتحديات التي تواجهها.

إن تحديد حجم العينة وإجراءات جمع البيانات يُسهم في تعزيز موثوقية النتائج. إن وجود خطة واضحة لجمع البيانات وتحليلها يسهل من عملية تفسير النتائج ويُعزز من قابلية التطبيق العملي للتوصيات الناتجة عن البحث. من خلال هذا الفصل، سيتمكن الباحثون من تقديم دراسة شاملة تسهم في تعزيز الأمن السيبراني في المؤسسات الحكومية، وتقديم رؤى عملية للمسؤولين وصانعي القرار حول كيفية تحسين استراتيجيات الحماية والتخفيف.

المنهجية وطرق البحث

تعد المنهجية الكمية أداة رئيسية في دراسة تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية، حيث تتيح تحليل البيانات بطريقة علمية وموضوعية لدعم الفرضيات وتقديم رؤى دقيقة حول الاستراتيجيات الأكثر فعالية للحماية والتخفيف. تعنى المنهجية الكمية بجمع وتحليل البيانات الرقمية من خلال أدوات وأساليب إحصائية، مما يوفر قاعدة قوية لفهم العلاقات بين المتغيرات وتقييم فعالية الاستراتيجيات الأمنية. في هذا السياق، تتضمن المنهجية الكمية عدة مراحل وخطوات أساسية تشمل تصميم الدراسة، جمع البيانات، تحليل البيانات، وتفسير النتائج.

تصميم الدراسة هو المرحلة الأولى والأكثر أهمية في المنهجية الكمية، حيث يتعين تحديد الأهداف البحثية، وصياغة الفرضيات، واختيار الأدوات المناسبة لجمع البيانات. في دراسة تقييم مخاطر الأمن السيبراني، يبدأ التصميم بتحديد الأهداف البحثية المحددة التي تسعى الدراسة إلى تحقيقها، مثل تقييم فعالية استراتيجيات الحماية الحالية، أو تحليل مدى استعداد المؤسسات الحكومية للتعامل مع المخاطر السيبرانية.

بعد تحديد الأهداف، يتم صياغة الفرضيات التي ستختبر خلال البحث. الفرضيات قد تشمل مثلاً: "تطبيق استراتيجيات الحماية السيبرانية المتقدمة يقلل بشكل كبير من المخاطر السيبرانية في المؤسسات الحكومية"، أو "التدريب والتوعية المستمرة للموظفين يعزز من فعالية استراتيجيات الأمن السيبراني". تستند هذه الفرضيات إلى الأدبيات السابقة والمعرفة النظرية حول الأمن السيبراني.

اختيار أدوات جمع البيانات هو خطوة حاسمة في التصميم. تشمل الأدوات الشائعة في المنهجية الكمية الاستبيانات، والمقاييس الرقمية، والبيانات الثانوية. في هذا السياق، يمكن استخدام الاستبيانات لتجميع بيانات من موظفي المؤسسات الحكومية حول ممارسات الأمن السيبراني والإجراءات المتبعة، بينما توفر البيانات الثانوية تحليلات سابقة أو تقارير تتعلق بالحوادث السيبرانية وأداء استراتيجيات الحماية.

جمع البيانات هو المرحلة الثانية في المنهجية الكمية، ويشمل تنفيذ الأدوات التي تم تحديدها في مرحلة التصميم. يمكن أن يتم جمع البيانات من خلال عدة طرق، مثل إرسال الاستبيانات إلى موظفي المؤسسات الحكومية، أو إجراء مقابلات structured مع المسؤولين عن الأمن السيبراني في هذه المؤسسات. الهدف من جمع البيانات هو الحصول على معلومات دقيقة وشاملة حول المخاطر السيبرانية والتدابير المتخذة لتخفيفها.

تتضمن عملية جمع البيانات في دراسة تقييم مخاطر الأمن السيبراني تنظيم الاستبيانات بحيث تتناول جميع جوانب الأمن السيبراني، مثل الأساليب المستخدمة للحماية، والتدريب، والاستجابة للحوادث. قد تشمل الاستبيانات أسئلة متعددة الخيارات، وأسئلة تقييم، وأسئلة مفتوحة للحصول على معلومات نوعية. من الضروري التأكد من أن الاستبيانات مصممة بطريقة تمكن من الحصول على بيانات قابلة للتحليل الإحصائي.

تحليل البيانات هو المرحلة التي يتم فيها تحويل البيانات الخام إلى معلومات ذات معنى وقيمة. في المنهجية الكمية، يتضمن التحليل استخدام أدوات إحصائية لفحص العلاقات بين المتغيرات واختبار الفرضيات. يمكن استخدام برامج التحليل الإحصائي مثل SPSS، أو R، أو Python لتحليل البيانات.

تبدأ عملية التحليل بتقييم جودة البيانات وتنظيفها، وهو خطوة ضرورية لضمان دقة النتائج. يشمل التنظيف إزالة البيانات غير الصحيحة أو المفقودة، وضمان تطابق البيانات مع معايير البحث. بعد التنظيف، يتم تطبيق الأساليب الإحصائية مثل التحليل الوصفي لتلخيص البيانات واختبار الفرضيات باستخدام التحليل الاستدلالي.

تشمل الأساليب الإحصائية الشائعة في تحليل بيانات الأمن السيبراني تحليل الانحدار لتحديد مدى تأثير المتغيرات المستقلة مثل استراتيجيات الحماية على المتغير التابع مثل مستوى المخاطر، وتحليل التباين لتحديد الفروقات بين مجموعات مختلفة مثل المؤسسات التي تطبق استراتيجيات حماية متقدمة مقابل تلك التي لا تطبقها.

تفسير النتائج هو المرحلة التي يتم فيها استخدام نتائج التحليل للإجابة على الأسئلة البحثية وتقييم الفرضيات. في دراسة تقييم مخاطر الأمن السيبراني، يتطلب تفسير النتائج ربط البيانات التي تم تحليلها بالسياق النظري والعملي للبحث. يتضمن ذلك فهم كيف تعكس النتائج فعالية استراتيجيات الحماية والتخفيف المستخدمة في المؤسسات الحكومية، ومدى استعدادها للتعامل مع التهديدات السيبرانية.

يتضمن تفسير النتائج أيضاً مقارنة النتائج التي تم الحصول عليها مع الأبحاث السابقة والنظريات ذات الصلة. يمكن أن تساعد هذه المقارنة في تحديد ما إذا كانت الاستراتيجيات الحالية فعالة أم تحتاج إلى تعديل. كما يمكن أن توفر التفسيرات رؤى حول المجالات التي تتطلب تحسينات، وتساعد في تطوير توصيات قائمة على البيانات لتحسين الأمن السيبراني.

المرحلة الأخيرة في المنهجية الكمية تتضمن تقديم التوصيات بناءً على نتائج البحث. يتم إعداد تقارير مفصلة تلخص النتائج الرئيسية، وتقدم توصيات لتحسين استراتيجيات الحماية والتخفيف من المخاطر السيبرانية. تشمل هذه التوصيات تحسين السياسات الأمنية، وتحديث الإجراءات الحالية، وتعزيز برامج التدريب والتوعية. تتضمن التقارير أيضاً تحليل الفجوات بين الممارسات الحالية والمعايير المثلى للأمن السيبراني. يمكن أن تساعد هذه التقارير المؤسسات الحكومية في تحديد الأولويات، وتوجيه الموارد بشكل أكثر فعالية لتعزيز الأمان السيبراني.

توفر المنهجية الكمية إطاراً منهجياً وشاملاً لتحليل وتقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية. من خلال تصميم الدراسة بشكل دقيق، وجمع البيانات بفعالية، وتحليلها باستخدام أساليب إحصائية متقدمة، وتفسير النتائج بشكل منهجي، يمكن الحصول على رؤى قيمة تساعد في تطوير استراتيجيات الحماية والتخفيف من المخاطر السيبرانية. تعزز هذه المنهجية من القدرة على تقديم توصيات مبنية على البيانات لتحسين الأمن السيبراني وضمان حماية فعالة للمعلومات والأنظمة في المؤسسات الحكومية.

مجتمع البحث

يمثل مجتمع البحث الفئة المستهدفة من الأفراد أو المؤسسات التي يتم جمع البيانات منها من أجل تحليل المخاطر المتعلقة بالأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية. يُعتبر تحديد مجتمع البحث خطوة حاسمة في أي دراسة، حيث يحدد نطاق البحث ويمكّن الباحثين من تحليل المعلومات بشكل دقيق وموثوق. في هذه الدراسة، سيتناول مجتمع البحث المؤسسات الحكومية المختلفة، بما في ذلك الوزارات والهيئات الحكومية، مما يُعكس تنوع التحديات التي تواجه الأمن السيبراني في السياق الحكومي.

- تحديد مجتمع البحث

يتكون مجتمع البحث من مجموعة متنوعة من المؤسسات الحكومية التي تشمل وزارات، مثل وزارة الداخلية، ووزارة التعليم، ووزارة الصحة، ووزارات أخرى تُعنى بتقديم الخدمات العامة. هذه المؤسسات تمثل قطاعات مختلفة من الحكومة، مما يُتيح دراسة متكاملة تشمل مجموعة واسعة من التحديات والمخاطر السيبرانية. يُعتبر هذا التنوع ضرورياً لفهم كيف تؤثر طبيعة كل مؤسسة على مستوى تعرضها للمخاطر السيبرانية. سيتم تضمين موظفين من مختلف

المستويات الإدارية والتخصصات الفنية، مما يعكس تنوع الخبرات والآراء حول قضايا الأمن السيبراني. يشمل ذلك موظفين من إدارات تقنية المعلومات، ومديري الأمن، والموظفين التنفيذيين، مما يُتيح جمع معلومات شاملة حول الاستراتيجيات المعتمدة ومدى وعي الأفراد بالمخاطر.

- أهمية تنوع مجتمع البحث

تتجلى أهمية تنوع مجتمع البحث في أنه يوفر قاعدة بيانات غنية تُعزز من مصداقية النتائج. من خلال دراسة مجموعة متنوعة من المؤسسات الحكومية، يمكن للباحثين تحليل كيفية تأثير العوامل المختلفة على مخاطر الأمن السيبراني. كما يُمكن أن تكشف الاختلافات بين المؤسسات عن الاستراتيجيات الأكثر فعالية في حماية البيانات والمعلومات.

هذا التنوع أيضًا يُساعد في فهم كيف يمكن أن تؤثر الثقافات التنظيمية المختلفة على مستوى الوعي بمخاطر الأمن السيبراني. فبينما قد تتبنى بعض المؤسسات استراتيجيات أمان متقدمة، قد تظل أخرى تتعامل مع القضايا بطريقة تقليدية. من خلال دراسة هذه الفروق، يمكن أن تُستخلص توصيات مُخصصة لتحسين الأمن السيبراني في المؤسسات المختلفة.

- تحديد حدود مجتمع البحث

يجب تحديد حدود مجتمع البحث بشكل واضح لتفادي أي تداخل قد يؤثر على دقة النتائج. في هذه الدراسة، ستركز البيانات على المؤسسات الحكومية داخل المملكة العربية السعودية، مع استبعاد المؤسسات الخاصة أو غير الربحية. كما سيتم تحديد فترة زمنية لجمع البيانات، مما يساعد في ضمان موثوقية المعلومات.

من المهم أيضًا توضيح أن المجتمع البحثي سيكون محدودًا بمجموعة من العوامل، مثل حجم المؤسسة، ونوع الخدمات التي تقدمها، ومدى تعرضها للمخاطر السيبرانية. يساعد هذا في تحديد نطاق البحث بشكل دقيق ويضمن التركيز على الجوانب الأكثر أهمية.

- خطوات جمع البيانات من مجتمع البحث

سيتضمن جمع البيانات من مجتمع البحث استخدام أدوات متعددة مثل الاستبيانات والمقابلات. سيتم تصميم الاستبيانات بعناية لتتناسب مع احتياجات كل فئة من فئات الموظفين، مع التركيز على جمع معلومات دقيقة حول الوعي بالمخاطر، والممارسات الأمنية المتبعة، والموارد المتاحة. كما يمكن أن تُجرى مقابلات مع مديري الأمن ورؤساء إدارات تقنية المعلومات للحصول على رؤى أعمق حول كيفية تقييمهم للمخاطر السيبرانية واستراتيجيات الحماية المعتمدة. هذه الخطوات ستُساعد في الحصول على بيانات غنية تُعزز من نتائج البحث.

- أهمية دراسة مجتمع البحث

إن دراسة مجتمع البحث في هذه الدراسة تعكس أهمية التوجهات الحالية في الأمن السيبراني، وتهدف إلى توفير فهم عميق للمخاطر التي تواجه المؤسسات الحكومية في المملكة. من خلال التركيز على المجتمع الحكومي، يمكن أن تسهم هذه الدراسة في تطوير استراتيجيات فعالة لتخفيف المخاطر وتعزيز الحماية.

كما ستوفر نتائج الدراسة رؤى قيّمة لصانعي القرار والجهات المعنية في الحكومة، مما يعزز من فعالية السياسات الأمنية ويضمن حماية المعلومات الحساسة. إن فهم مجتمع البحث بشكل دقيق يُساعد أيضاً في وضع توصيات مستندة إلى البيانات، مما يزيد من قابلية تطبيقها في الواقع العملي. يُعتبر مجتمع البحث عنصراً أساسياً في دراسة تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية، حيث يسهم في تقديم نتائج موثوقة ورؤى عملية تُساعد في تحسين الأمن السيبراني وحماية المعلومات في المملكة العربية السعودية.

محددات حجم العينة:

تمثل محددات حجم العينة عنصراً حيوياً في تصميم أي دراسة بحثية، حيث تحدد عدد الأفراد أو الوحدات التي سيتم دراستها لجمع البيانات اللازمة. في إطار هذه الدراسة، التي تركز على تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية، فإن اختيار حجم العينة المناسب يصبح ضرورياً لتحقيق نتائج دقيقة وموثوقة. يتناول هذا الجزء من الدراسة مجموعة من المحددات التي تؤثر على حجم العينة، والتي تشمل الاعتبارات الإحصائية، والموارد المتاحة، وطبيعة المجتمع المستهدف، وغيرها من العوامل.

- الاعتبارات الإحصائية

تُعتبر الاعتبارات الإحصائية من أبرز العوامل المؤثرة في تحديد حجم العينة. يعتمد حجم العينة المثالي على عدة معايير إحصائية، مثل مستوى الثقة، والهامش المقبول للخطأ. عادةً ما تُستخدم مستويات ثقة تبلغ 95% أو 99%، حيث يعني ذلك أن الباحثين يتوقعون أن تكون النتائج قريبة جداً من الواقع.

يُعتمد أيضاً على حجم العينة لتقليل الهامش الخطأ، والذي يمثل الفرق بين القيمة الحقيقية في المجتمع والقيمة التي يتم تقديرها من العينة. لذا، كلما زاد حجم العينة، زاد مستوى الثقة في النتائج. ومع ذلك، فإن زيادة حجم العينة تتطلب موارد إضافية وتكاليف أكبر، مما يستدعي تحقيق توازن بين دقة النتائج والموارد المتاحة.

- طبيعة المجتمع المستهدف

طبيعة المجتمع المستهدف تلعب دوراً مهماً في تحديد حجم العينة. في هذه الدراسة، يتم استهداف مجموعة من المؤسسات الحكومية التي تختلف في حجمها ونوع الخدمات التي تقدمها. يتطلب ذلك أن يكون حجم العينة مناسباً لتمثيل تنوع المؤسسات المختلفة، حيث إن بعض الوزارات قد تضم عدداً كبيراً من الموظفين، بينما قد تكون هيئات أخرى أصغر في الحجم.

لذلك، يجب أن يتم تحديد حجم العينة بطريقة تعكس هذا التنوع، مما يُمكن الباحثين من الحصول على بيانات تعبر عن كل جانب من جوانب المجتمع. يمكن استخدام أساليب أخذ العينات الطبقية أو العشوائية لضمان تمثيل كافة الفئات بشكل عادل.

- الموارد المتاحة

تُعتبر الموارد المتاحة أحد العوامل الحاسمة في تحديد حجم العينة. يشمل ذلك الميزانية، والوقت، والموارد البشرية المتاحة لجمع البيانات. فعلى سبيل المثال، إذا كانت الميزانية المحددة للدراسة محدودة، فقد يتعين على الباحثين تقليل حجم العينة أو استخدام أساليب أكثر كفاءة لجمع البيانات.

كما يؤثر الوقت المتاح لإجراء البحث على حجم العينة، حيث أن جمع البيانات من عينة كبيرة قد يتطلب وقتاً أطول. وبالتالي، من المهم تحديد حجم العينة بما يتناسب مع المدة الزمنية المحددة للدراسة، دون التأثير على جودة البيانات المتاحة.

- أهداف الدراسة

يجب أيضاً مراعاة أهداف الدراسة عند تحديد حجم العينة. في حالة دراسة تقييم مخاطر الأمن السيبراني، قد يكون الهدف هو الحصول على بيانات شاملة حول مدى الوعي بالمخاطر واستراتيجيات الحماية المتبعة. في هذه الحالة، يمكن أن يتطلب الأمر عينة أكبر لضمان شمول كافة الآراء والتوجهات.

بينما إذا كان الهدف هو تحليل ظاهرة معينة أو مقارنة محددة بين فئات معينة من المؤسسات، فقد يكون حجم العينة أقل، ولكن يجب أن يكون ممثلاً للمجتمع بشكل دقيق. يُعتبر فهم أهداف الدراسة جزءاً أساسياً من تحديد حجم العينة بشكل صحيح.

- خطوات تحديد حجم العينة

تتضمن خطوات تحديد حجم العينة عدة إجراءات، مثل:

1. تحديد المجتمع المستهدف: يبدأ الأمر بتحديد المجتمع الذي سيتم جمع البيانات منه بوضوح، مما يساعد في فهم طبيعة العينة المطلوبة.
2. تحديد مستوى الثقة والهامش الخطأ: يُحدد الباحثون مستوى الثقة المطلوب، على أن يُحدد أيضاً الهامش المقبول للخطأ.
3. حساب حجم العينة: يُستخدم عدد من الصيغ الإحصائية لحساب حجم العينة بناءً على المعلومات المتاحة.
4. التأكد من التمثيل: يُراجع الباحثون العينة للتأكد من أنها تمثل تنوع المجتمع بشكل جيد، وقد يُعدل حجم العينة بناءً على ذلك.

- أهمية تحديد حجم العينة بدقة

إن تحديد حجم العينة بدقة يعتبر أمراً بالغ الأهمية لضمان موثوقية النتائج. فحجم العينة غير الكافي يمكن أن يؤدي إلى نتائج مضللة، مما يؤثر سلباً على الاستنتاجات والتوصيات الناتجة عن البحث. من خلال ضمان أن تكون العينة مناسبة، يستطيع الباحثون تعزيز مصداقية البحث وزيادة ثقة صانعي القرار في النتائج.

يعكس اختيار حجم العينة الجيد مستوى الاحترافية والالتزام العلمي للباحثين، مما يساهم في تعزيز جودة الدراسة ككل. لذا، فإن الاعتبارات المذكورة أعلاه تساهم في تحديد حجم عينة يعكس واقع الأمن السيبراني في المؤسسات الحكومية، مما يضمن نتائج دقيقة وقابلة للتطبيق في الواقع العملي.

خطوات جمع البيانات:

تُعتبر خطوات جمع البيانات جزءًا أساسيًا من أي دراسة بحثية، حيث تحدد كيفية الحصول على المعلومات اللازمة لتحقيق أهداف البحث. في إطار هذه الدراسة، التي تركز على تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية، يتم اتخاذ عدة خطوات منهجية لجمع البيانات. تهدف هذه الخطوات إلى ضمان جودة المعلومات ودقتها، مما يساهم في تعزيز موثوقية النتائج والاستنتاجات.

1. تحديد أهداف جمع البيانات

تبدأ خطوات جمع البيانات بتحديد الأهداف الواضحة للعملية. يجب أن تكون هذه الأهداف متوافقة مع أهداف البحث العام، مثل تقييم المخاطر السيبرانية، وفهم استراتيجيات الحماية الحالية، ومدى وعي الموظفين بالمخاطر. من خلال تحديد الأهداف، يتمكن الباحثون من توجيه عملية جمع البيانات بشكل فعال، مما يساعد في توضيح أنواع البيانات المطلوبة.

2. اختيار أدوات جمع البيانات

بعد تحديد الأهداف، تأتي مرحلة اختيار أدوات جمع البيانات المناسبة. في هذه الدراسة، سيتم استخدام مجموعة من الأدوات، منها:

✓ الاستبيانات: تُعتبر الاستبيانات أداة فعالة لجمع البيانات من عدد كبير من المشاركين. سيتم تصميم استبيان يتضمن مجموعة من الأسئلة المتعلقة بالمخاطر السيبرانية، واستراتيجيات الحماية، ومدى الوعي بالمخاطر. سيتم استخدام أسئلة مغلقة، مثل اختيار من بين خيارات محددة، بالإضافة إلى أسئلة مفتوحة تسمح للمشاركين بالتعبير عن آرائهم وتجاربهم بشكل حر.

✓ المقابلات: تُستخدم المقابلات للحصول على رؤى أعمق حول الموضوع من الأفراد ذوي الخبرة. يمكن أن تشمل المقابلات مديري الأمن، ورؤساء أقسام تقنية المعلومات، وغيرهم من المعنيين بالأمن السيبراني. توفر هذه الأداة فرصة للتفاعل المباشر مع المشاركين، مما يعزز من دقة المعلومات المجمعة.

✓ الملاحظات المباشرة: قد تُستخدم الملاحظات المباشرة في بعض الحالات لمراقبة كيفية تطبيق استراتيجيات الحماية في المؤسسات. توفر هذه الطريقة فرصة لفهم السياق الذي تُدار فيه العمليات الأمنية.

3. إعداد الاستبيانات والمقابلات

يتطلب إعداد الاستبيانات والمقابلات الاهتمام بتفاصيل دقيقة. يجب أن تكون الأسئلة واضحة وسهلة الفهم، مع تجنب أي مصطلحات تقنية قد تكون غير مألوفة للمشاركين. سيتم إجراء اختبارات تجريبية (Pilot Testing) على الاستبيانات والمقابلات مع مجموعة صغيرة من الأفراد لضمان وضوح الأسئلة وملاءمتها.

تشمل عملية الإعداد أيضًا تحديد كيفية توزيع الاستبيانات، سواء عبر البريد الإلكتروني أو من خلال وسائل التواصل الاجتماعي أو من خلال اللقاءات الشخصية. في حالة المقابلات، يجب تحديد الجدول الزمني وتنسيق المواعيد مع المشاركين لضمان حصول الباحثين على الوقت الكافي لجمع المعلومات.

4. جمع البيانات

تبدأ المرحلة الرئيسية من جمع البيانات بعد إعداد الأدوات. سيتم إرسال الاستبيانات إلى المشاركين عبر القنوات المحددة، مع توفير تعليمات واضحة حول كيفية ملء الاستبيانات. يفضل استخدام منصة إلكترونية لجمع البيانات، حيث تتيح هذه المنصات تجميع البيانات بشكل منظم وتسهيل عملية التحليل لاحقًا.

في حالة المقابلات، ستُجرى اللقاءات في بيئة مريحة تتيح للمشاركين التعبير عن آرائهم بحرية. سيتم تسجيل المقابلات (بعد الحصول على إذن المشاركين) لتسهيل عملية التحليل لاحقًا، مما يساعد في ضمان دقة المعلومات.

5. مراقبة جودة البيانات

خلال عملية جمع البيانات، من المهم مراقبة جودة البيانات التي يتم جمعها. يجب أن يكون هناك نظام للتأكد من أن المشاركين يملؤون الاستبيانات بشكل دقيق، وأن المقابلات تتم بطريقة منظمة. في حالة وجود أي مشكلات، مثل عدم استكمال الاستبيانات أو غموض في الإجابات، يجب اتخاذ الإجراءات المناسبة لمعالجة هذه المشكلات.

يمكن أيضًا استخدام تقنيات استقصائية مثل متابعة المشاركين لتأكيد صحة المعلومات المقدمة. هذا يساهم في تحسين جودة البيانات التي يتم جمعها ويزيد من موثوقيتها.

6. تحليل البيانات

بعد جمع البيانات، تأتي مرحلة تحليلها. ستُستخدم أدوات تحليل البيانات الإحصائية لتحليل النتائج المستخلصة من الاستبيانات والمقابلات. يتضمن ذلك تصنيف البيانات، واستخدام الأساليب الإحصائية لاستخراج الأنماط والاتجاهات. سيساعد هذا التحليل على تقييم المخاطر السيبرانية وفهم كيفية تأثيرها على المؤسسات الحكومية.

7. توثيق العملية

من المهم توثيق جميع خطوات جمع البيانات بشكل دقيق. يُعزز هذا التوثيق من مصداقية البحث ويساعد في مراجعة العملية لاحقًا. يجب أن تشمل الوثائق معلومات حول المشاركين، وأدوات جمع البيانات، وأي ملاحظات أو تعليقات تم الحصول عليها خلال العملية.

8. تقييم نتائج جمع البيانات

بعد الانتهاء من جمع وتحليل البيانات، يجب تقييم النتائج. يتضمن ذلك مراجعة البيانات المستخلصة من الاستبيانات والمقابلات والتأكد من أنها تتماشى مع الأهداف المحددة للدراسة. يجب أن تُسلط الضوء على أهم النتائج التي تم الحصول عليها، وكيفية تأثيرها على الفهم العام لمخاطر الأمن السيبراني في المؤسسات الحكومية.

✓ أهمية خطوات جمع البيانات

تُعتبر خطوات جمع البيانات أمرًا حاسمًا في نجاح أي دراسة. فهي تضمن الحصول على معلومات دقيقة وموثوقة، مما يساهم في تعزيز نتائج البحث والاستنتاجات التي يتم التوصل إليها. من خلال اتباع خطوات منهجية ومنظمة، يمكن للباحثين تقديم نتائج تدعم تحسين استراتيجيات الحماية والتخفيف في المؤسسات الحكومية، مما يساهم في تعزيز الأمن السيبراني في المملكة العربية السعودية.

حدود البحث

✓ الحدود البشرية

تعتبر الحدود البشرية من العوامل الرئيسية التي تحدد نطاق الدراسة، حيث تشير إلى الفئات والأفراد المشاركين في البحث. في دراسة تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية، يتم تحديد الحدود البشرية بناءً على الأشخاص الذين يتعاملون مباشرة مع الأمن السيبراني في هذه المؤسسات. تشمل الفئات الرئيسية المستهدفة في هذه الدراسة المسؤولين عن إدارة الأمن السيبراني، مديري تكنولوجيا المعلومات، فرق الاستجابة للحوادث السيبرانية، وأيضاً الموظفين الذي يتعاملون مع أنظمة المعلومات بشكل يومي.

التركيز على هذه الفئات يتيح الحصول على رؤى شاملة حول فعالية الاستراتيجيات الأمنية المطبقة، كما أن إشراك هؤلاء الأفراد يمكن أن يوفر معلومات قيمة حول تحديات تطبيق السياسات الأمنية ومستوى الوعي بممارسات الأمن السيبراني. الحدود البشرية تشمل كذلك تحديد معايير اختيار المشاركين، مثل الخبرة العملية في مجال الأمن السيبراني، ودرجة المسؤولية في المؤسسة، لضمان جمع بيانات دقيقة وموثوقة تعكس واقع الأوضاع الأمنية.

✓ الحدود الزمانية

الحدود الزمانية تشير إلى الفترة الزمنية التي تُجرى فيها الدراسة، والتي تلعب دوراً مهماً في تحديد سياق النتائج وتفسيرها. في دراسة تقييم مخاطر الأمن السيبراني، يتم تحديد الفترة الزمنية بناءً على متطلبات البحث والأهداف المرجوة. عادةً ما تتضمن الدراسة فترة زمنية محددة لجمع البيانات وتحليلها، تقع هذه الفترة من أكتوبر 2023 حتى يوليو 2024م.

الاهتمام بالحدود الزمانية يضمن التناسق في جمع البيانات وتحليلها، كما يتيح فرصة لملاحظة التغيرات في الأوضاع الأمنية والتقنيات المستخدمة بمرور الوقت. على سبيل المثال، قد تتغير استراتيجيات الأمن السيبراني وتطور التقنيات المستخدمة في الحماية بشكل مستمر، لذا من الضروري تحديد فترة زمنية مناسبة لمراقبة هذه التغيرات وتقييم تأثيرها على فعالية الأمان السيبراني.

✓ الحدود المكانية

الحدود المكانية تتعلق بالموقع الجغرافي الذي تُجرى فيه الدراسة، وتحدد نطاق المؤسسات التي سيتم فحصها في البحث. في هذه الدراسة، تركز الحدود المكانية على المؤسسات الحكومية في المملكة العربية السعودية، وهذا يشمل مختلف

الجهات الحكومية التي تمتلك أنظمة معلومات حساسة والتي تحتاج إلى تقييم استراتيجيات الحماية والتخفيف من المخاطر السيبرانية.

الحدود المكانية تشمل أيضًا اختيار المؤسسات التي ستتم دراسة الأمن السيبراني فيها، مثل الوزارات، الهيئات الحكومية، والوكالات العامة. من المهم تحديد المواقع الجغرافية بدقة لضمان أن الدراسة تعكس التنوع في المؤسسات الحكومية من حيث حجمها ونوعها وأنواع التهديدات التي قد تواجهها. تشمل الحدود المكانية أيضًا التعرف على اختلافات بين المناطق المختلفة في المملكة، مثل المدن الكبرى مقابل المناطق الريفية، لضمان أن النتائج تمثل الواقع الأمني السيبراني بشكل شامل.

الفصل الرابع

نتائج الدراسة

المقدمة

يمثل الفصل الرابع من هذه الدراسة نقطة الانطلاق نحو فهم النتائج العملية والتحليلات المستندة إلى البيانات التي تم جمعها. يتناول هذا الفصل تحليل البيانات، ونتائج البحث، والتوصيات المستندة إلى هذه النتائج. يُعتبر هذا الفصل جوهر البحث، حيث يهدف إلى تقديم رؤية واضحة حول الوضع الحالي للأمن السيبراني في المؤسسات الحكومية بالمملكة، مما يساهم في تطوير استراتيجيات فعالة لحماية المعلومات وضمان استمرارية الأعمال.

سيبدأ هذا الفصل بتوضيح كيفية إجراء تحليل البيانات التي تم جمعها خلال البحث. يعتمد تحليل البيانات على استخدام أساليب إحصائية ووصفية تُمكن الباحثين من تفسير المعلومات بشكل دقيق. سيتم استخدام برامج تحليل البيانات المختلفة لمعالجة المعلومات وتحليلها، مما يسهل استخراج الأنماط والاتجاهات المهمة. سيتناول التحليل أيضًا تقييم علاقة المتغيرات المستقلة (مثل التدريب الكافي وتحديث البرمجيات وتقنيات التشفير) بالمتغير التابع (مخاطر الأمن السيبراني).

يُعتبر تحليل البيانات خطوة حاسمة، حيث يتيح للباحثين فهم مدى تأثير العوامل المختلفة على مستوى المخاطر. كما يوفر أساسًا قويًا لاستنتاجات الدراسة، مما يضمن موثوقية النتائج. من خلال تحليل البيانات بشكل منهجي، سيتمكن الباحثون من تقديم صورة دقيقة عن المخاطر التي تواجهها المؤسسات الحكومية والتحديات المتعلقة بالأمن السيبراني. بعد تحليل البيانات، سيتناول الفصل عرض النتائج التي تم التوصل إليها. ستشمل النتائج تفاصيل حول مستوى المخاطر السيبرانية التي تواجهها المؤسسات الحكومية، بالإضافة إلى الفروق بين المؤسسات في كيفية تعاملها مع هذه المخاطر. سيتم أيضًا تقديم البيانات بشكل مرئي، مثل الرسوم البيانية والجداول، لعرض النتائج بطريقة تسهل فهمها. يعتبر عرض النتائج أمرًا أساسيًا في البحث، حيث يتيح للقارئ فهم الحالة الحالية للأمن السيبراني. من خلال تقديم النتائج بشكل دقيق وشامل، سيتمكن الباحثون من توضيح مدى فعالية الاستراتيجيات الحالية ووجود نقاط الضعف في النظام الأمني. كما تعكس النتائج مدى جاهزية المؤسسات الحكومية لمواجهة التهديدات السيبرانية وكيفية تعاملها معها.

سيتناول هذا الفصل التوصيات المستندة إلى النتائج التي تم تحليلها. بناءً على النتائج التي تم الوصول إليها، سيتم تقديم مجموعة من التوصيات العملية التي يمكن أن تتبناها المؤسسات الحكومية لتعزيز أمنها السيبراني. تشمل هذه التوصيات تعزيز برامج التدريب، وتطوير سياسات تحديث البرمجيات، وتحسين تقنيات التشفير المستخدمة.

تُعتبر التوصيات جزءًا حيويًا من البحث، حيث تهدف إلى تقديم حلول عملية قابلة للتنفيذ. من خلال تقديم هذه التوصيات، يسعى الباحثون إلى تمكين صانعي القرار من اتخاذ خطوات فعالة لتحسين الأمن السيبراني، مما يساهم في حماية المعلومات الحساسة وضمان استمرارية الأعمال. كما تعكس التوصيات التوجهات المستقبلية في مجال الأمن السيبراني، مما يساعد المؤسسات الحكومية على الاستعداد للتحديات القادمة.

إن تناول تحليل البيانات، والنتائج، والتوصيات في هذا الفصل يُعد أمرًا بالغ الأهمية لتوجيه الجهود نحو تحسين الأمن السيبراني في المؤسسات الحكومية. يُعتبر تحليل البيانات الأساس الذي يُبنى عليه جميع الاستنتاجات والتوصيات، حيث يُساعد في فهم التحديات والتهديدات الحالية. كما أن عرض النتائج بشكل واضح يُعزز من شفافية البحث ويساهم في إطلاع المعنيين على الحالة الراهنة للأمن السيبراني.

إن تقديم توصيات عملية يُساهم في تسهيل عملية اتخاذ القرار، مما يمكن المؤسسات الحكومية من تعزيز استراتيجياتها الأمنية. يُظهر هذا الفصل كيف يمكن للبحث الأكاديمي أن يُساهم بشكل فعال في معالجة قضايا معقدة مثل الأمن السيبراني، وبالتالي تعزيز الأمان في الفضاء الرقمي للمملكة العربية السعودية. من خلال هذا الفصل، سيتمكن الباحثون من تقديم مساهمة قيمة في تطوير سياسات الأمن السيبراني وضمان حماية المعلومات الحساسة في المؤسسات الحكومية.

تحليل البيانات

• الوصف الإحصائي للبيانات

- ما هو الإحصاء الوصفي؟

يستخدم الإحصاء الوصفي لتحديد الخصائص الأساسية لنتائج الدراسة، وهو يوفر ملخصات سريعة للعينة والمقاييس، هم أساس أي تحليل بيانات كمي عملياً، إلى جانب تحليل الرسومات الأساسية.

في معظم الحالات، يُفضل الإبلاغ عن الإحصائيات الخاصة بك بطريقة مباشرة في مقالتك، عند الاستشهاد بعدة إحصائيات حول نفس الموضوع، من الأفضل القيام بذلك في جملة أو فقرة معينة.

- ما الغرض من الإحصاء الوصفي؟

في كل مجال من مجالات الحياة، يعد الإحصاء الوصفي أمراً بالغ الأهمية، صمم كل تحليل إحصائي لمساعدتك في اكتساب فهم شامل للمتغيرات في بحثك.

هناك العديد من أغراض الإحصاء الوصفي، منها:

- استخدام الإحصائيات الوصفية لوصف البيانات الكمية بطريقة منطقية ومفهومة.
- قد يكون لدينا الكثير من القياسات في تقرير بحثي، بدلاً من ذلك، يمكننا تقييم عدد كبير من الأشخاص باستخدام أي عملية.
- تساعدنا الإحصاءات الوصفية في فهم كميات هائلة من البيانات، إذ تقوم كل إحصائية وصفية بتكثيف كمية كبيرة من المعلومات في وصف موجز.

Statistics						
Std. Error of Kurtosis	Kurtosis	Std. Error of Skewness	Skewness	Std. Deviation	N	

					Valid	
0.260	-1.302	0.130	-0.032	1.416	351	العمر
0.260	-1.917	0.130	-0.307	0.495	351	الجنس
0.260	-1.312	0.130	0.003	1.430	351	الدرجة
0.260	-1.415	0.130	0.049	1.474	351	يعتبر الأمن السيبراني أولوية رئيسية في المؤسسات الحكومية.
0.260	-1.290	0.130	0.008	1.400	351	توفر المؤسسات الحكومية تدريباً كافياً للموظفين حول ممارسات الأمن السيبراني.
0.260	-1.264	0.130	0.017	1.411	351	توجد سياسات واضحة لمواجهة التهديدات السيبرانية في المؤسسات الحكومية.
0.260	-1.258	0.130	0.028	1.401	351	يتم تحديث البرمجيات والتطبيقات بشكل دوري لحماية البيانات الحساسة.
0.260	-1.362	0.130	-0.053	1.461	351	تجرى تقييمات دورية للمخاطر السيبرانية في المؤسسات الحكومية.

0.260	-1.288	0.130	0.044	1.429	351	تُستخدم تقنيات التشفير لحماية البيانات الحساسة في المؤسسات.
0.260	-1.174	0.130	-0.142	1.357	351	توجد خطط استجابة واضحة لحالات الطوارئ السيبرانية.
0.260	-1.257	0.130	-0.093	1.411	351	يتم تشجيع الموظفين على الإبلاغ عن أي تهديدات تتعلق بالأمن السيبراني.
0.260	-1.420	0.130	0.042	1.470	351	تشجع المؤسسات الحكومية الابتكار في تقنيات الأمن السيبراني.
0.260	-1.243	0.130	0.057	1.395	351	مستوى الأمن السيبراني في المؤسسات يلبي الاحتياجات الحالية.
0.260	-1.237	0.130	0.002	1.354	351	تقيم المؤسسات أداء مزودي خدمات الأمن السيبراني بشكل دوري.
0.260	-1.350	0.130	0.096	1.440	351	توجد ثقافة مؤسسية تدعم الأمن السيبراني بين جميع الموظفين.

0.260	-1.236	0.130	-0.008	1.378	351	تستخدم أدوات فعالة لرصد التهديدات السيبرانية في المؤسسات.
0.260	-1.363	0.130	-0.113	1.441	351	تعتبر الإجراءات المتخذة لحماية البيانات كافية في المؤسسات الحكومية.
0.260	-1.192	0.130	0.005	1.353	351	يشارك جميع الموظفين في جهود تعزيز الأمن السيبراني.
0.260	-1.269	0.130	-0.083	1.398	351	تدعم الميزانية المخصصة للأمن السيبراني في المؤسسات الحكومية.
0.260	-1.321	0.130	0.030	1.414	351	توجد آليات لتبادل المعلومات حول التهديدات السيبرانية بين المؤسسات.

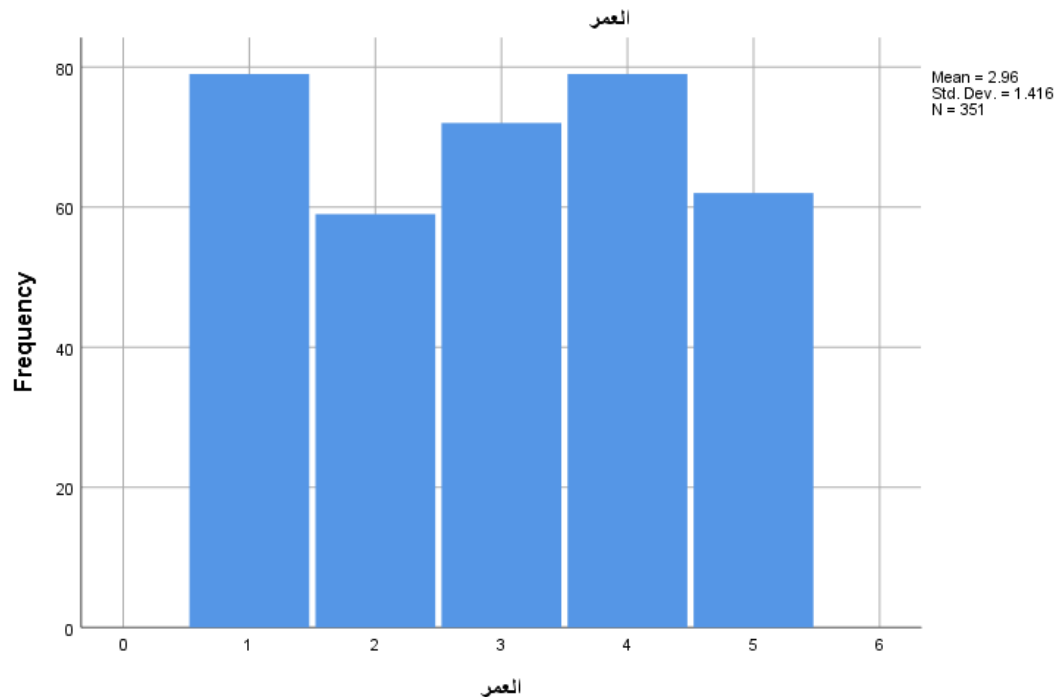
جدول 1: الوصف الاحصائي للبيانات.

1. سن المشاركين

تظهر نتائج الدراسة أن الفئة العمرية الأكثر مشاركة في تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية تتراوح ما بين 20-30 عاماً و50-60 عاماً، وذلك بنسبة 22.5%. تعكس هذه النسبة أعلى مستوى من المشاركة بين الفئات العمرية، مما يدل على أهمية وعي الشباب وخبرة الأفراد الأكبر سناً في قضايا الأمن السيبراني. الفئة العمرية من 20 إلى 30 عاماً تمثل الجيل الذي نشأ في عصر التكنولوجيا الرقمية، مما يمكنهم من فهم التحديات والتهديدات السيبرانية بشكل أفضل، ويؤهلهم للعب دور فعال في تطوير استراتيجيات الحماية. بينما يمثل الأفراد من 50 إلى 60 عاماً خبرة مهنية معمقة ومعرفة عميقة حول المخاطر التاريخية والتغيرات التي طرأت على مجالات الأمن. هذه التركيبة السكانية المتنوعة قد تساهم في تقديم رؤى متعددة الجوانب حول المخاطر السيبرانية، مما يعكس الحاجة الملحة لوضع استراتيجيات فعالة للتخفيف من تلك المخاطر في المؤسسات الحكومية. بشكل عام، يُظهر توازن المشاركة بين الفئات العمرية أهمية التعاون بين الأجيال المختلفة لتعزيز الأمن السيبراني، حيث يمكن أن تسهم الخبرة والحيوية في تطوير حلول مبتكرة وشاملة لمواجهة التحديات الحالية والمستقبلية.

سن المشاركين					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	20-30	79	22.5	22.5	22.5
	30-40	59	16.8	16.8	39.3
	40-50	72	20.5	20.5	59.8
	50-60	79	22.5	22.5	82.3
	60+	62	17.7	17.7	100.0
	Total	351	100.0	100.0	

جدول 2: الوصف الإحصائي لعمر المشاركين في التجربة.



رسم توضيحي 2: التمثيل البياني لعمر المشاركين في التجربة.

2. جنس المشاركين

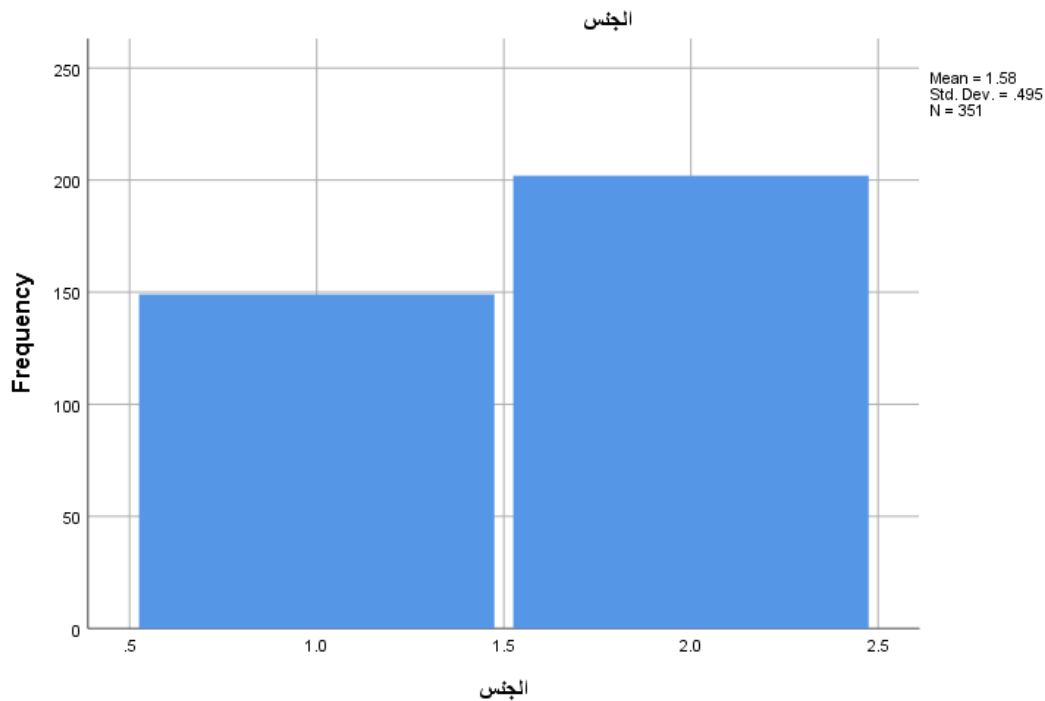
تشير النتائج إلى أن الذكور كانوا الأكثر مشاركة في الدراسة حول تقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية، حيث بلغت نسبة مشاركتهم 22.5%. تعكس هذه النسبة تفضيلاً ملحوظاً للذكور في المشاركة في هذا الموضوع الحيوي، مما قد يدل على عدة عوامل. أولاً، يمكن أن يكون هناك اهتمام أكبر بين الذكور بالمجالات التقنية والتكنولوجية، مما يزيد من رغبتهم في المشاركة في تقييم قضايا الأمن السيبراني. ثانياً، قد ترتبط هذه النسبة بوجود عدد أكبر من الذكور في مجالات العمل المتعلقة بتكنولوجيا المعلومات والأمن السيبراني داخل المؤسسات الحكومية، حيث يُعتبر هذا المجال تقنياً بشكل رئيسي ويستقطب غالباً الأفراد من الجنس الذكري.

يمكن أن تكون الثقافة السائدة في المجتمع السعودي تلعب دوراً في تعزيز مشاركة الذكور في مثل هذه الدراسات، حيث يتم تشجيعهم على الانخراط في المجالات التقنية والمهنية. من المهم أيضاً ملاحظة أن هذا الاختلال في التوزيع قد يؤثر على النتائج النهائية للدراسة، حيث قد لا تعكس آراء الإناث، مما يعزز الحاجة إلى تشجيع مشاركة أكبر من جميع الفئات،

وخاصة الإناث، لضمان شمولية الرؤى والتوجهات حول الأمن السيبراني. وبالتالي، فإن فهم الديناميات بين الجنسين في هذا المجال يمكن أن يساعد في تصميم استراتيجيات أفضل وأكثر شمولية لمواجهة التحديات المرتبطة بالأمن السيبراني.

جنس المشاركون					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أنثى	149	42.5	42.5	42.5
	ذكر	202	57.5	57.5	100.0
	Total	351	100.0	100.0	

جدول 3: الوصف الإحصائي لجنس المشاركين.



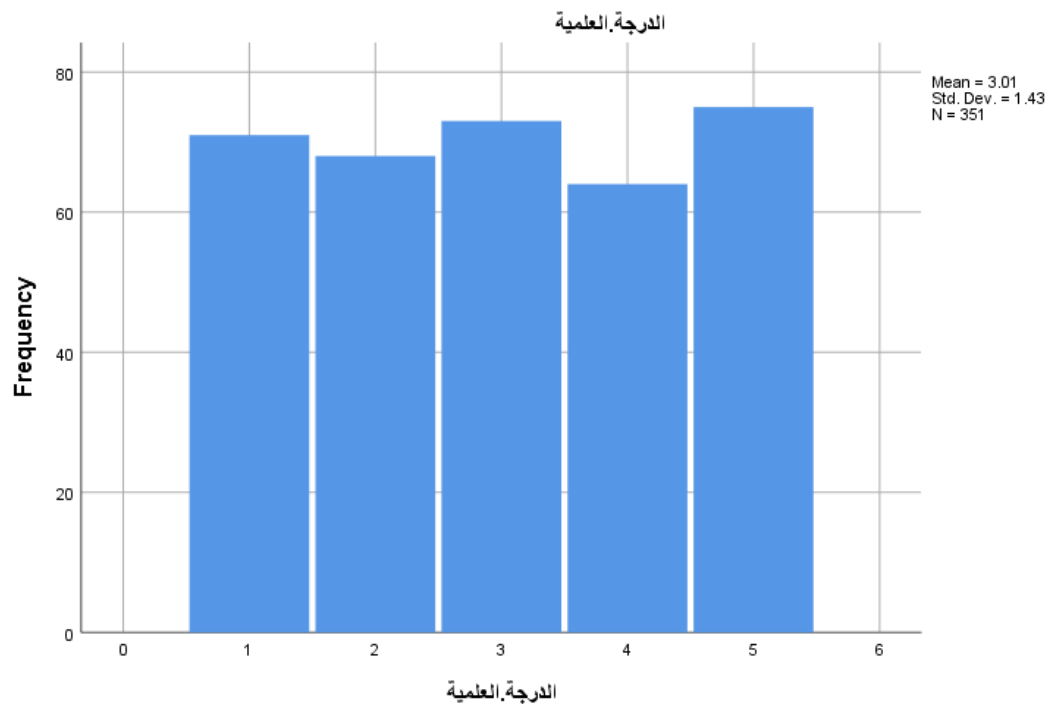
رسم توضيحي 3: التمثيل البياني لجنس المشاركين

3. الدرجة العلمية للمشاركين

تشير النتائج إلى أن الحاصلين على شهادة الدراسات العليا هم الأكثر مشاركة في الدراسة المتعلقة بتقييم مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية، حيث بلغت نسبة مشاركتهم 20.8%. يعكس ذلك اهتمامًا متزايدًا من قبل الأفراد ذوي الخلفيات الأكاديمية المتقدمة بقضايا الأمن السيبراني، مما يدل على أنهم يمتلكون الوعي الكافي حول المخاطر والتهديدات المحتملة التي تواجه المؤسسات الحكومية. قد يكون هذا الوعي ناتجًا عن التعليم المتخصص الذي حصلوا عليه، والذي يُمكنهم من فهم تعقيدات الأمن السيبراني وأهمية استراتيجيات الحماية والتخفيف. كما أن مشاركة هذه الفئة بشكل ملحوظ تشير إلى أهمية إشراك الخبراء الأكاديميين والمهنيين في تطوير السياسات والبرامج التي تهدف إلى تعزيز الأمن السيبراني، مما قد يسهم في تحسين فعالية هذه السياسات في مواجهة التحديات الأمنية. بالتالي، تُعتبر هذه النسبة بمثابة مؤشر على الحاجة إلى تعزيز التعاون بين المؤسسات الحكومية والأكاديميين لضمان تطوير استراتيجيات فعالة تلبي احتياجات ومتطلبات الأمن السيبراني في البلاد.

الدرجة العلمية للمشاركين					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	درجة البكالوريوس	71	20.2	20.2	20.2
	دكتوراه	68	19.4	19.4	39.6
	شهادة الدراسة الثانوية	73	20.8	20.8	60.4
	شهادة عليا	64	18.2	18.2	78.6
	ماجستير	75	21.4	21.4	100.0
	Total	351	100.0	100.0	

جدول 4: الوصف الاحصائي لدرجة العلمية للمشاركين.



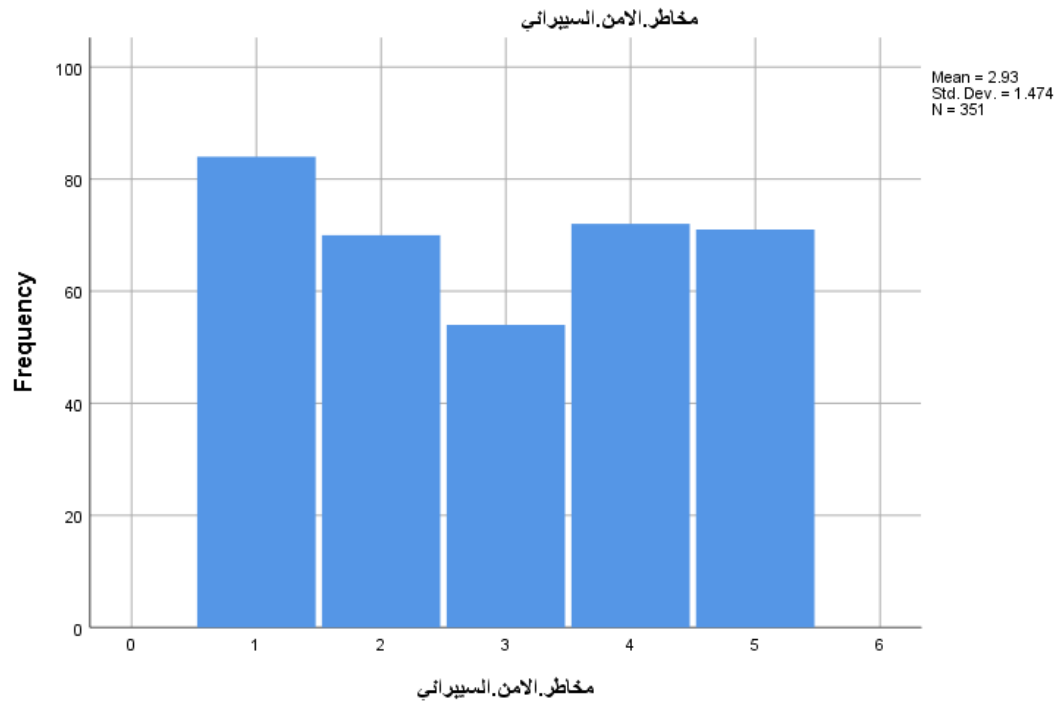
رسم توضيحي 4: التمثيل البياني لدرجة العلمية للمشاركين.

4. يعتبر الأمن السيبراني أولوية رئيسية في المؤسسات الحكومية.

تشير النسبة التي أظهرتها استجابات المشاركين، والتي بلغت 23.9% من المشاركين الذين أكدوا على أن الأمن السيبراني يعتبر أولوية رئيسية في المؤسسات الحكومية، إلى وعي متزايد بأهمية حماية المعلومات والأنظمة الرقمية في ظل التهديدات المتزايدة التي تواجهها هذه المؤسسات. يعكس هذا الاتجاه إدراكًا عميقًا للآثار السلبية التي يمكن أن تترتب على انتهاكات الأمن السيبراني، مثل فقدان البيانات الحساسة، وتضرر السمعة، وزيادة التكاليف المتعلقة بالاستجابة للحوادث الأمنية. كما تشير هذه النسبة إلى ضرورة تعزيز استراتيجيات الحماية والتخفيف لضمان سلامة العمليات الحكومية، مما يستدعي استثمارًا أكبر في تقنيات الأمان، وتدريب الموظفين، وتطوير سياسات أمنية فعالة. علاوة على ذلك، يعكس هذا الوعي أهمية التنسيق بين الجهات الحكومية المختلفة لتعزيز الدفاعات السيبرانية، مما يساهم في بناء ثقة المواطنين في الخدمات الحكومية والقدرة على التعامل مع التحديات الرقمية. في المجمل، تدل هذه النسبة على أن الأمن السيبراني أصبح جزءًا لا يتجزأ من استراتيجيات العمل الحكومي، مما يؤكد الحاجة الملحة لتطوير إطار عمل شامل يعزز من الاستجابة لتلك التهديدات ويضمن استمرارية الأعمال الحكومية بفعالية وكفاءة.

يعتبر الأمن السيبراني أولوية رئيسية في المؤسسات الحكومية					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أوافق	84	23.9	23.9	23.9
	أوافق بشدة	70	19.9	19.9	43.9
	لا أوافق	54	15.4	15.4	59.3
	لا أوافق بشدة	72	20.5	20.5	79.8
	لا أوافق ولا أرفض	71	20.2	20.2	100.0
	Total	351	100.0	100.0	

جدول 5: الوصف الاحصائي لاعتبار الأمن السيبراني أولوية رئيسية في المؤسسات الحكومية.



رسم توضيحي 5: التمثيل البياني لاعتبار الأمن السيبراني أولوية رئيسية في المؤسسات الحكومية

5. توفر المؤسسات الحكومية تدريباً كافياً للموظفين حول ممارسات الأمن السيبراني.

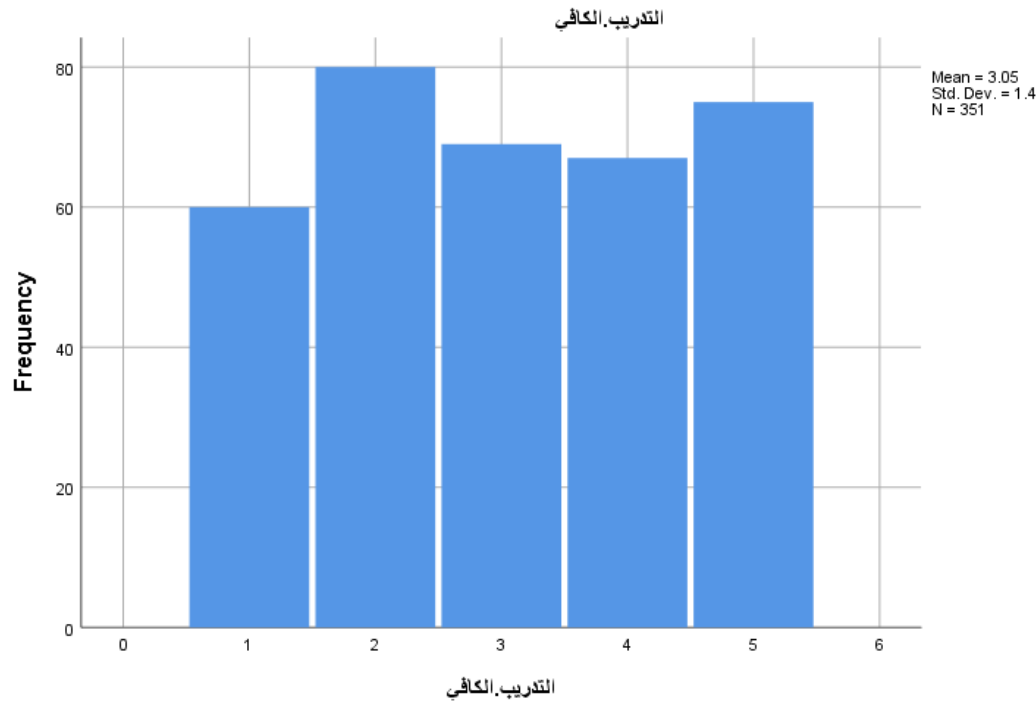
تشير نسبة 22.8% من المشاركين الذين أكدوا بشدة على أن المؤسسات الحكومية توفر تدريباً كافياً للموظفين حول ممارسات الأمن السيبراني إلى إدراك متزايد لأهمية التعليم والتوعية في مجال الحماية من التهديدات السيبرانية. هذه النسبة تعكس الاعتراف بأن العنصر البشري يعد أحد العوامل الرئيسية التي تؤثر على فعالية استراتيجيات الأمن السيبراني، حيث يمكن أن تؤدي الأخطاء البشرية إلى اختراقات خطيرة. لذا، فإن توفير التدريب الكافي للموظفين يمثل خطوة حيوية في تعزيز الثقافة الأمنية داخل المؤسسات الحكومية، مما يساهم في تحسين مستوى الوعي لدى الموظفين حول التهديدات المحتملة وكيفية التعامل معها بفعالية.

تشير هذه النسبة إلى التزام المؤسسات الحكومية بتطوير سياسات أمنية شاملة تتضمن التدريب المستمر، مما يعكس رغبة قوية في بناء بيئة عمل آمنة وموثوقة. هذا التدريب لا يقتصر فقط على التعرف على التهديدات، بل يتضمن أيضاً كيفية تطبيق أفضل الممارسات في الأمن السيبراني، مثل إدارة كلمات المرور، واستخدام التقنيات الأمنية الحديثة، والتعامل مع الحوادث بشكل فعال. وفي نهاية المطاف، يُظهر هذا التركيز على التدريب استجابة المؤسسات الحكومية

للتحديات المتزايدة في الفضاء السيبراني، مما يساعد على تعزيز قدرة هذه المؤسسات على حماية المعلومات الحساسة
وضمان استمرارية العمليات الحكومية بشكل آمن وفعال.

توفر المؤسسات الحكومية تدريباً كافياً للموظفين حول ممارسات الأمن السيبراني					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أوافق	60	17.1	17.1	17.1
	أوافق بشدة	80	22.8	22.8	39.9
	لا أوافق	69	19.7	19.7	59.5
	لا أوافق بشدة	67	19.1	19.1	78.6
	لا أوافق ولا أرفض	75	21.4	21.4	100.0
	Total	351	100.0	100.0	

جدول 6: الوصف الاحصائي لتوفر المؤسسات الحكومية تدريباً كافياً للموظفين حول ممارسات الأمن السيبراني.



رسم توضيحي 6: التمثيل البياني لتوفر المؤسسات الحكومية تدريباً كافياً للموظفين حول ممارسات الأمن السيبراني

6. توجد سياسات واضحة لمواجهة التهديدات السيبرانية في المؤسسات الحكومية.

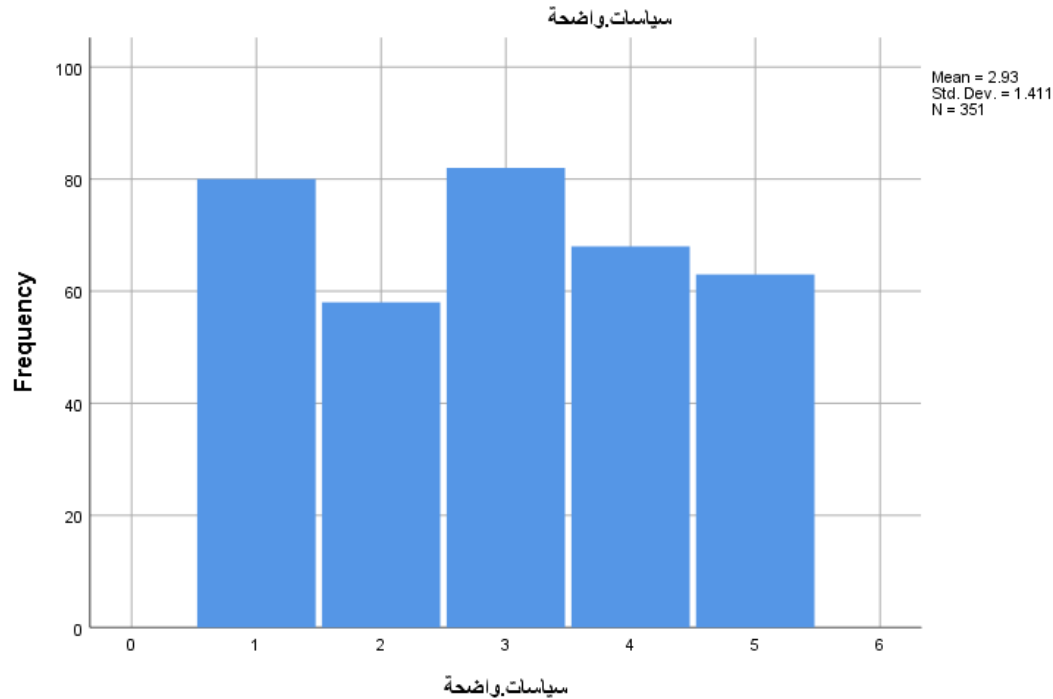
تشير نسبة 22.8% من المشاركين الذين أكدوا وجود سياسات واضحة لمواجهة التهديدات السيبرانية في المؤسسات الحكومية إلى وعي متزايد بأهمية وضع استراتيجيات محددة للتصدي للمخاطر المحتملة في الفضاء السيبراني. هذه النسبة تعكس التزام المؤسسات الحكومية بتطوير أطر عمل قوية تعزز من قدرتها على التصدي للتهديدات المتزايدة التي تواجهها، خاصة في ظل الاعتماد المتزايد على التكنولوجيا في تقديم الخدمات الحكومية. وجود سياسات واضحة يعد خطوة أساسية نحو تحسين مستوى الأمان السيبراني، حيث يمكّن المؤسسات من تحديد المخاطر المحتملة، ووضع آليات استجابة فعالة، وتحديد الأدوار والمسؤوليات لجميع المعنيين.

إن هذه السياسات لا تقتصر على مجرد وجودها على الورق، بل تعكس أيضاً التوجه نحو تكامل الأمن السيبراني ضمن الثقافة المؤسسية. إن وجود سياسات موحدة يساعد في تنسيق الجهود بين مختلف الإدارات والأقسام، مما يساهم في تحقيق استجابة أكثر فاعلية تجاه التهديدات. كما يشير ذلك إلى وجود إيمان بضرورة مواجهة التحديات بشكل استباقي، مما يعكس تحسّن مستوى الوعي السيبراني بين الموظفين وصناع القرار في المؤسسات الحكومية. بالتالي، فإن هذه النسبة

تعتبر مؤشراً إيجابياً على اتجاه المؤسسات الحكومية نحو تحسين مستويات الأمان وحماية البيانات، مما يعزز من الثقة في الخدمات المقدمة ويعزز الأمن العام في المجتمع.

توجد سياسات واضحة لمواجهة التهديدات السيبرانية في المؤسسات الحكومية					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أوافق	80	22.8	22.8	22.8
	أوافق بشدة	58	16.5	16.5	39.3
	لا أوافق	82	23.4	23.4	62.7
	لا أوافق بشدة	68	19.4	19.4	82.1
	لا أوافق ولا أرفض	63	17.9	17.9	100.0
	Total	351	100.0	100.0	

جدول 7: الوصف الإحصائي لوجود سياسات واضحة لمواجهة التهديدات السيبرانية في المؤسسات الحكومية.



رسم توضيحي 7: التمثيل البياني لوجود سياسات واضحة لمواجهة التهديدات السيبرانية في المؤسسات الحكومية

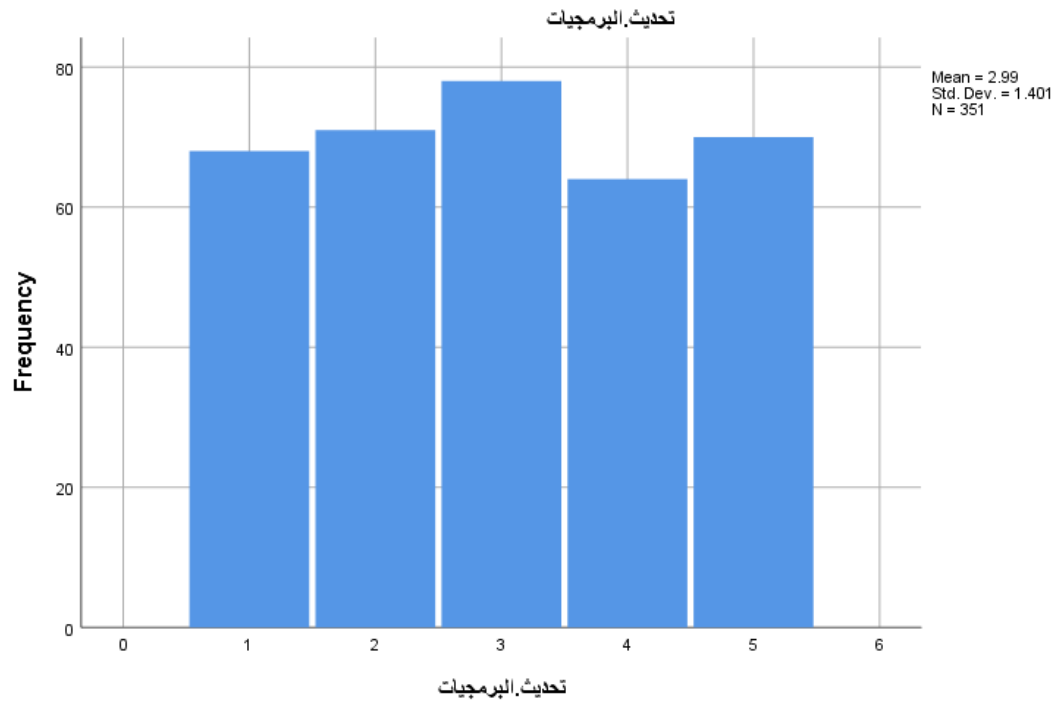
7. يتم تحديث البرمجيات والتطبيقات بشكل دوري لحماية البيانات الحساسة.

تشير نسبة 22.2% من المشاركين الذين أعربوا عن عدم موافقتهم على أن البرمجيات والتطبيقات تُحدث بشكل دوري لحماية البيانات الحساسة إلى وجود ضعف واضح في استراتيجيات الأمان السيبراني المتبعة في المؤسسات الحكومية، مما يعكس احتمالية تعرض هذه المؤسسات لمخاطر جسيمة تتعلق بالاختراق وسرقة المعلومات. هذه النسبة تبرز قلقاً كبيراً حول فعالية الإجراءات الحالية لحماية البيانات، حيث أن عدم التحديث الدوري للبرمجيات يُعد بمثابة ثغرة استراتيجية يمكن أن تُستغل من قبل المهاجمين، مما يُشدد على الحاجة الماسة لتقييم سياسات الأمان وتحديثها بانتظام لمواكبة التهديدات المتطورة. من المهم أن يُدرك الموظفون أهمية الصيانة الدورية للتطبيقات والبرمجيات، حيث أن هذا يتطلب التزاماً واضحاً من الإدارة بضرورة توفير التدريب والموارد اللازمة لتعزيز ثقافة الأمان السيبراني، وتطبيق سياسات صارمة تضمن استجابة فعالة لأي تهديدات قد تطرأ. بالإضافة إلى ذلك، فإن هذه النسبة العالية من عدم الموافقة تشير إلى انعدام الثقة في الأمان الرقمي المتوفر، مما قد يؤثر سلباً على الروح المعنوية للموظفين وكفاءتهم في أداء واجباتهم،

ويستدعي بالتالي الحاجة إلى استراتيجية شاملة تحسن من ممارسات الأمان السيبراني، وتضمن حماية فعالة للبيانات الحساسة في المؤسسات الحكومية.

يتم تحديث البرمجيات والتطبيقات بشكل دوري لحماية البيانات الحساسة					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أوافق	68	19.4	19.4	19.4
	أوافق بشدة	71	20.2	20.2	39.6
	لا أوافق	78	22.2	22.2	61.8
	لا أوافق بشدة	64	18.2	18.2	80.1
	لا أوافق ولا أرفض	70	19.9	19.9	100.0
	Total	351	100.0	100.0	

جدول 8: الوصف الاحصائي لتحديث البرمجيات والتطبيقات بشكل دوري لحماية البيانات الحساسة.



رسم توضيحي 8: التمثيل البياني لتحديث البرمجيات والتطبيقات بشكل دوري لحماية البيانات الحساسة

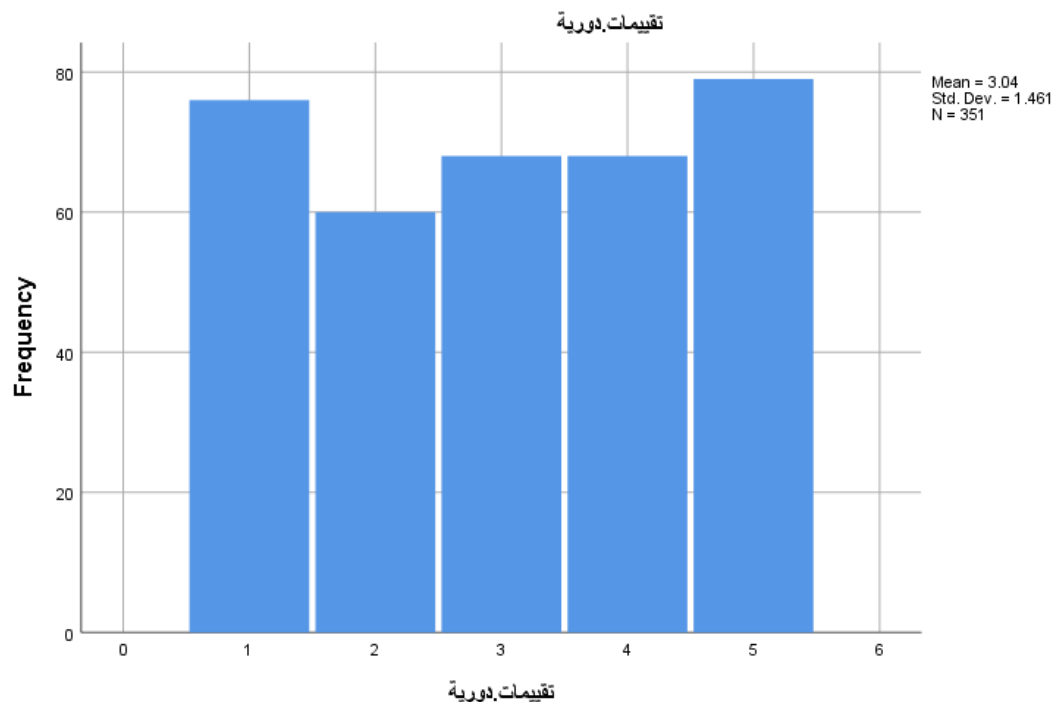
8. تجرى تقييمات دورية للمخاطر السيبرانية في المؤسسات الحكومية.

تشير نسبة 22.5% من المشاركين الذين أعربوا عن موقف "لا أوافق ولا أرفض" تجاه إجراء تقييمات دورية للمخاطر السيبرانية في المؤسسات الحكومية إلى حالة من عدم اليقين أو التردد بشأن فعالية السياسات الحالية في هذا المجال. هذه النسبة تعكس انعكاساً في الآراء، مما يشير إلى أن بعض المشاركين قد يرون ضرورة وجود تقييمات دورية للمخاطر السيبرانية كخطوة أساسية لضمان الأمان الرقمي، بينما قد يشعر آخرون بعدم وضوح أو قلة المعلومات حول ما إذا كانت هذه التقييمات تُجرى بالفعل بشكل منتظم. هذا التردد يمكن أن يُفهم في سياق أهمية الأمن السيبراني في حماية البيانات الحساسة والعمليات الحكومية، حيث أن التقييم الدوري هو جزء حيوي من أي استراتيجية أمان فعالة، يساعد على تحديد الثغرات المحتملة وتطوير استراتيجيات التخفيف. إذا كانت هذه التقييمات غير موجودة أو تُجرى بشكل غير كافٍ، فإن المؤسسات الحكومية قد تتعرض لمخاطر متزايدة، مما يستدعي الحاجة الملحة لتنفيذ الإجراءات اللازمة لضمان أن تكون التقييمات دورية، وموثوقة، وأن يتم توصيل نتائجها بوضوح لجميع المعنيين. في النهاية، إن تعزيز

الثقة في الأمان السيبراني يتطلب تحسين التواصل وتوفير الشفافية بشأن الإجراءات المتبعة، مما يساهم في تعزيز ثقافة الوعي الأمني داخل المؤسسات الحكومية.

تجربى تقييمات دورية للمخاطر السيبرانية في المؤسسات الحكومية					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أوافق	76	21.7	21.7	21.7
	أوافق بشدة	60	17.1	17.1	38.7
	لا أوافق	68	19.4	19.4	58.1
	لا أوافق بشدة	68	19.4	19.4	77.5
	لا أوافق ولا أرفض	79	22.5	22.5	100.0
	Total	351	100.0	100.0	

جدول 9: الوصف الاحصائي لتقييمات دورية للمخاطر السيبرانية في المؤسسات الحكومية.



رسم توضيحي 9: التمثيل البياني لتقييمات دورية للمخاطر السيبرانية في المؤسسات الحكومية

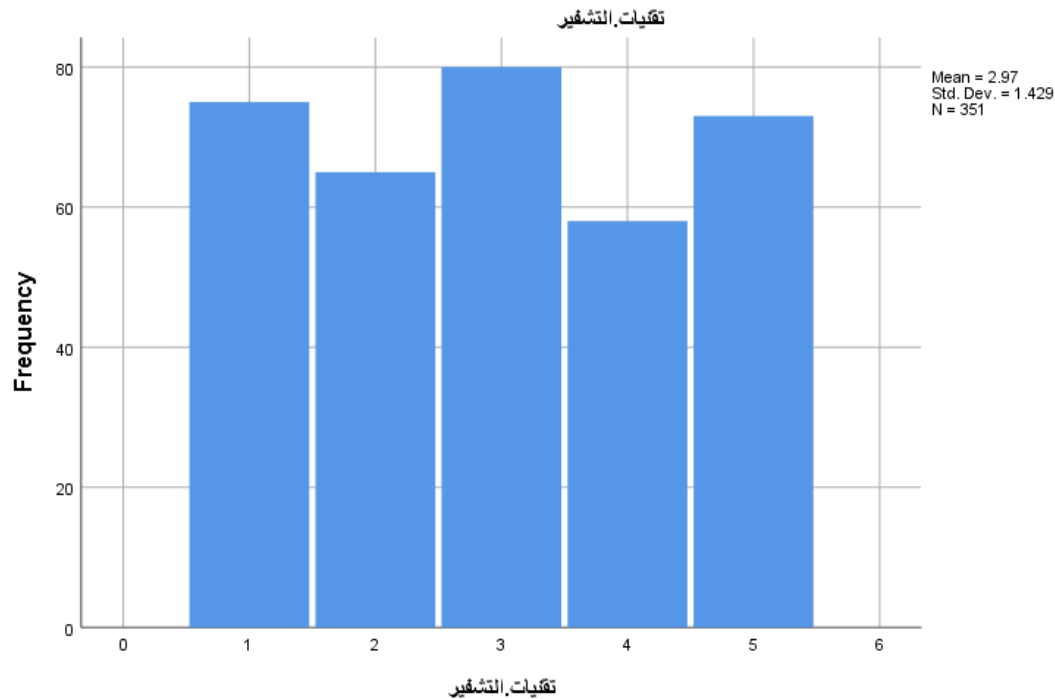
9. تُستخدم تقنيات التشفير لحماية البيانات الحساسة في المؤسسات.

تشير نسبة 22.8% من المشاركين الذين أعربوا عن عدم موافقتهم على استخدام تقنيات التشفير لحماية البيانات الحساسة في المؤسسات الحكومية إلى وجود قلق كبير بشأن فعالية تدابير الأمان السيبراني المتبعة. هذه النسبة العالية تعكس عدم الثقة في الإجراءات الأمنية الحالية، مما يدل على إمكانية وجود ثغرات في حماية المعلومات الحساسة التي تتعامل معها هذه المؤسسات. فالتشفير هو أحد الأدوات الأساسية التي تساعد على تأمين البيانات ومنع الوصول غير المصرح به إليها، وعندما يشعر عدد كبير من الموظفين بعدم وجوده، فإن ذلك يسלט الضوء على احتمال وجود نقص في الوعي أو المعرفة حول أهمية التشفير وطرق تطبيقه. كما يمكن أن يشير أيضاً إلى أن المؤسسات قد لا تستثمر بشكل كافٍ في التقنيات الضرورية أو أن هناك قصوراً في التدريب والتوجيه للموظفين حول كيفية استخدام هذه التقنيات بشكل فعال. إن عدم تطبيق التشفير بصورة صحيحة يمكن أن يؤدي إلى مخاطر جسيمة، مثل تسرب البيانات أو انتهاكات الخصوصية، مما يستدعي ضرورة إعادة تقييم استراتيجيات الأمان السيبراني في المؤسسات الحكومية. يتطلب

الأمر نهجاً أكثر شمولية، حيث ينبغي تعزيز الوعي والتدريب حول تقنيات التشفير، بالإضافة إلى اعتماد سياسات واضحة وصارمة تضمن حماية البيانات الحساسة بشكل فعال.

تُستخدم تقنيات التشفير لحماية البيانات الحساسة في المؤسسات					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أوافق	75	21.4	21.4	21.4
	أوافق بشدة	65	18.5	18.5	39.9
	لا أوافق	80	22.8	22.8	62.7
	لا أوافق بشدة	58	16.5	16.5	79.2
	لا أوافق ولا أرفض	73	20.8	20.8	100.0
	Total	351	100.0	100.0	

جدول 10: الوصف الاحصائي لاستخدام تقنيات التشفير لحماية البيانات الحساسة في المؤسسات.



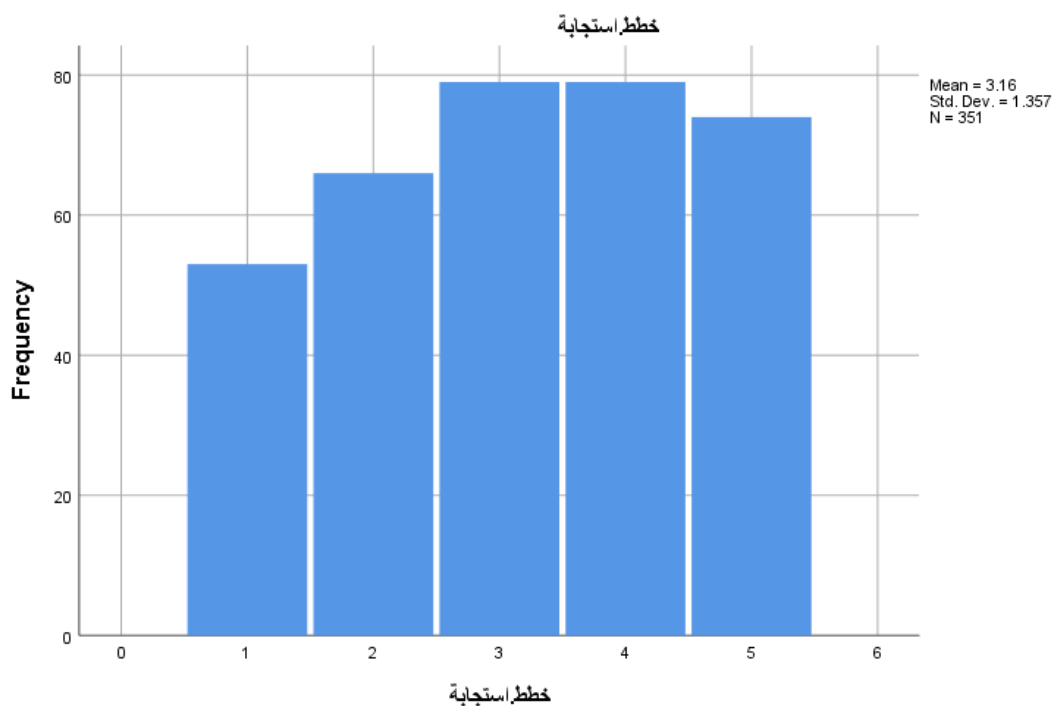
رسم توضيحي 10: التمثيل البياني لاستخدام تقنيات التشفير لحماية البيانات الحساسة في المؤسسات

10. توجد خطط استجابة واضحة لحالات الطوارئ السيبرانية.

تشير نسبة 22.5% من المشاركين الذين أعربوا عن عدم موافقتهم وعدم موافقتهم بشدة على وجود خطط استجابة واضحة لحالات الطوارئ السيبرانية إلى وجود ثغرة خطيرة في استراتيجيات الأمن السيبراني في المؤسسات الحكومية. هذه النسبة تمثل أعلى نسبة بين المشاركين، مما يدل على أن هناك شعوراً بالقلق وعدم الثقة في قدرة هذه المؤسسات على التعامل مع الأزمات السيبرانية بفعالية. عدم وجود خطط استجابة واضحة يعني أن المؤسسات قد تكون غير مستعدة لمواجهة الهجمات السيبرانية أو الحوادث التي قد تهدد أمن بياناتها، مما يزيد من خطر الأضرار المحتملة مثل فقدان البيانات الحساسة أو التعرض لانتهاكات الخصوصية. كما يشير ذلك إلى إمكانية عدم وجود تدريب كافٍ للموظفين على كيفية التصرف في حالات الطوارئ، مما قد يؤدي إلى استجابات غير فعالة أو متأخرة. من الضروري أن تقوم المؤسسات الحكومية بتطوير وتوثيق خطط استجابة شاملة، تشمل تقييم المخاطر، وتعزيز التواصل بين الفرق المعنية، وتقديم التدريب اللازم لضمان استعداد الموظفين. فوجود خطة استجابة فعالة يعد جزءاً أساسياً من أي استراتيجية للأمن السيبراني، ويعزز قدرة المؤسسات على حماية بياناتها وضمان استمرارية العمل في وجه التهديدات المتزايدة.

توجد خطط استجابة واضحة لحالات الطوارئ السيبرانية					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أوافق	53	15.1	15.1	15.1
	أوافق بشدة	66	18.8	18.8	33.9
	لا أوافق	79	22.5	22.5	56.4
	لا أوافق بشدة	79	22.5	22.5	78.9
	لا أوافق ولا أرفض	74	21.1	21.1	100.0
	Total	351	100.0	100.0	

جدول 11: الوصف الاحصائي لوجود خطط استجابة واضحة لحالات الطوارئ السيبرانية.



رسم توضيحي 11: التمثيل البياني لوجود خطط استجابة واضحة لحالات الطوارئ السيبرانية

11. يتم تشجيع الموظفين على الإبلاغ عن أي تهديدات تتعلق بالأمن السيبراني.

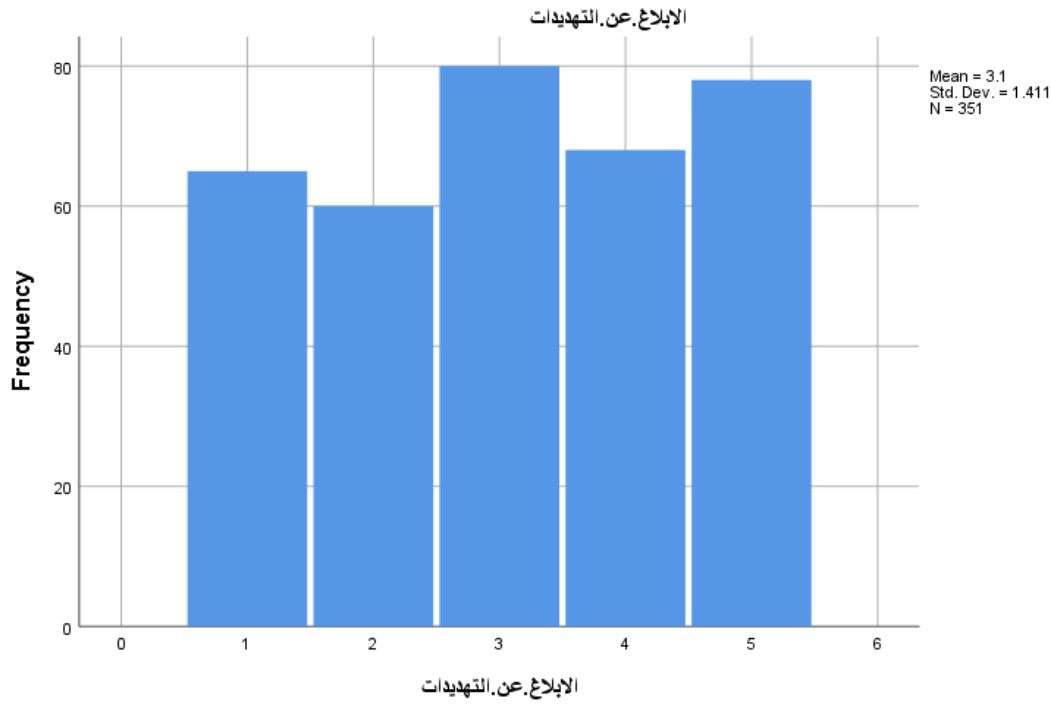
تشير نسبة 22.8% من المشاركين الذين أعربوا عن عدم موافقتهم على أن المؤسسات تشجع الموظفين على الإبلاغ عن أي تهديدات تتعلق بالأمن السيبراني إلى وجود فجوة كبيرة في ثقافة الأمن السيبراني داخل هذه المؤسسات. هذه النسبة العالية تعكس عدم شعور الموظفين بالراحة أو الأمان عند الإبلاغ عن التهديدات، مما قد يؤدي إلى تجاهل أو تقليل خطورة المشكلات الأمنية التي قد تكون لها آثار خطيرة على سلامة البيانات وأمن المعلومات. عدم تشجيع الموظفين على الإبلاغ يمكن أن يكون ناتجاً عن غياب التدريب المناسب أو التوعية بأهمية دورهم في حماية المؤسسة، بالإضافة إلى الخوف من العواقب السلبية التي قد تترتب على الإبلاغ، مثل المساءلة أو العقوبات.

عندما يشعر الموظفون بعدم الأمان في الإبلاغ عن المخاطر، فإن ذلك يؤدي إلى تقليص فعالية استراتيجيات الأمن السيبراني، حيث يُمكن أن يتسبب هذا في عدم اكتشاف التهديدات في وقت مبكر، مما يعرض البيانات والمعلومات الحساسة لخطر الهجمات أو الاختراقات. لذلك، من الضروري أن تعمل المؤسسات الحكومية على إنشاء بيئة عمل تشجع على الإبلاغ عن التهديدات، من خلال تطوير برامج تدريبية، وتقديم مكافآت للموظفين الذين يساهمون في تعزيز الأمن السيبراني، وتوفير قنوات آمنة وسرية للإبلاغ عن القضايا الأمنية. تعزيز هذه الثقافة سيساعد في تحسين الاستجابة للأزمات وتقوية الأمن السيبراني بشكل عام، مما يضمن حماية البيانات والمعلومات الحيوية للمؤسسة.

يتم تشجيع الموظفين على الإبلاغ عن أي تهديدات تتعلق بالأمن السيبراني					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أوافق	65	18.5	18.5	18.5
	أوافق بشدة	60	17.1	17.1	35.6
	لا أوافق	80	22.8	22.8	58.4
	لا أوافق بشدة	68	19.4	19.4	77.8

	لا أوافق ولا أرفض	78	22.2	22.2	100.0
	Total	351	100.0	100.0	

جدول 12: الوصف الاحصائي لتشجيع الموظفين على الإبلاغ عن أي تهديدات تتعلق بالأمن السيبراني



رسم توضيحي 12: الوصف الاحصائي لتشجيع الموظفين على الإبلاغ عن أي تهديدات تتعلق بالأمن السيبراني

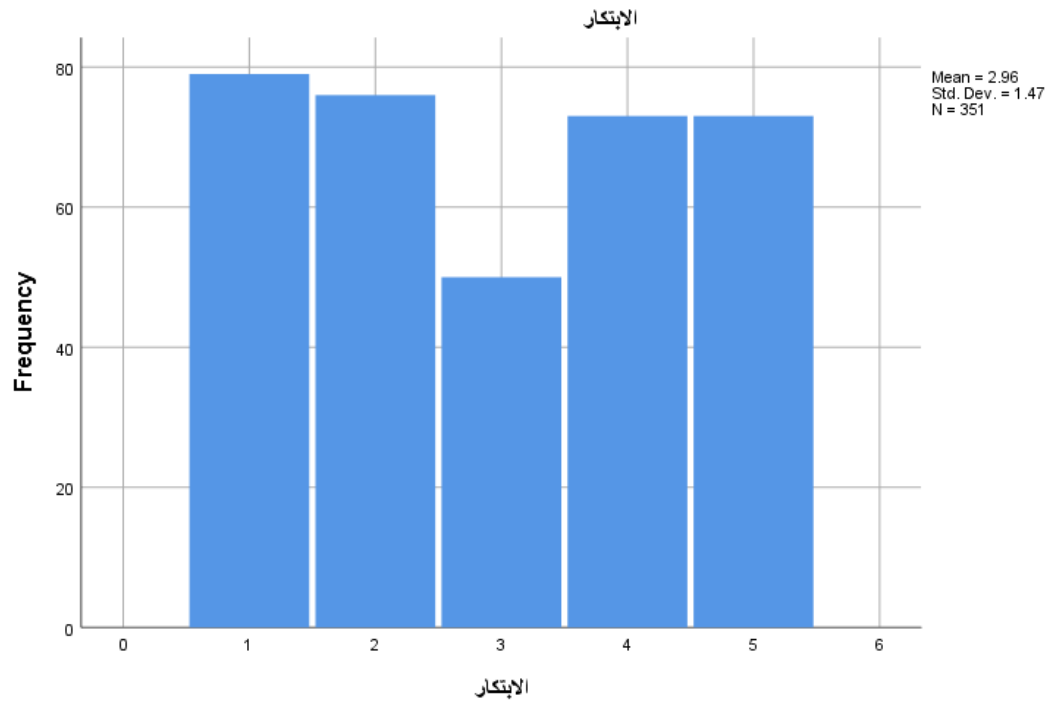
12. تشجع المؤسسات الحكومية الابتكار في تقنيات الأمن السيبراني.

تشير نسبة 22.5% من المشاركين الذين أكدوا أن المؤسسات الحكومية تشجع الابتكار في تقنيات الأمن السيبراني إلى وجود وعي متزايد بأهمية تطوير حلول جديدة وفعالة لمواجهة التهديدات السيبرانية المتنامية. هذه النسبة تعكس توجهاً إيجابياً نحو الابتكار، مما يدل على أن هناك إدراكاً لأهمية استخدام التقنيات الحديثة والأساليب الجديدة لتعزيز الأمن السيبراني. تشجيع الابتكار في هذا المجال يعد أمراً حيوياً، خاصةً في ظل التحديات المستمرة التي تواجه المؤسسات الحكومية، مثل زيادة عدد الهجمات السيبرانية وتعقيدها، والتي تتطلب استراتيجيات متطورة وفعالة.

من خلال دعم الابتكار، يمكن للمؤسسات الحكومية الاستفادة من التكنولوجيا الحديثة مثل الذكاء الاصطناعي وتحليل البيانات الكبيرة لتطوير نظم متقدمة للكشف عن التهديدات والاستجابة لها بشكل سريع. كما يمكن أن يسهم هذا التوجه في تعزيز التعاون بين الجهات الحكومية والشركات الناشئة والمبتكرين في مجال الأمن السيبراني، مما يؤدي إلى تبادل المعرفة والخبرات وتطوير حلول تتناسب مع احتياجات البيئة الحكومية. بالإضافة إلى ذلك، يعزز هذا النوع من الابتكار ثقة المواطنين في قدرة المؤسسات على حماية بياناتهم ومعلوماتهم الحساسة، مما يسهم في تحقيق أهداف الأمن السيبراني بشكل أكثر فعالية. لذا، يجب على هذه المؤسسات الاستمرار في تشجيع ثقافة الابتكار وتوفير الموارد اللازمة لدعم تطوير تقنيات جديدة، مما سيؤدي في النهاية إلى تحسين مستوى الأمان وحماية المعلومات في عصر يتسم بالتغير السريع.

تشجع المؤسسات الحكومية الابتكار في تقنيات الأمن السيبراني					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أوافق	79	22.5	22.5	22.5
	أوافق بشدة	76	21.7	21.7	44.2
	لا أوافق	50	14.2	14.2	58.4
	لا أوافق بشدة	73	20.8	20.8	79.2
	لا أوافق ولا أرفض	73	20.8	20.8	100.0
	Total	351	100.0	100.0	

جدول 13: الوصف الاحصائي لتشجيع المؤسسات الحكومية الابتكار في تقنيات الأمن السيبراني.



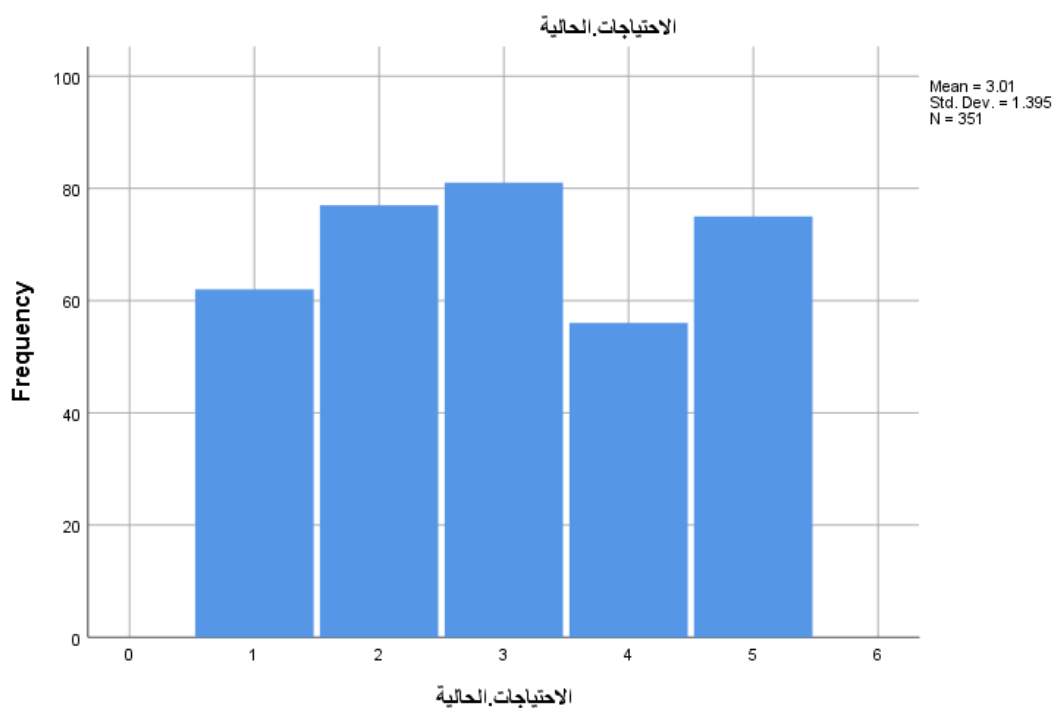
رسم توضيحي 13: التمثيل البياني لتشجيع المؤسسات الحكومية الابتكار في تقنيات الأمن السيبراني

13. مستوى الأمن السيبراني في المؤسسات يلي الاحتياجات الحالية.

تشير نسبة 23.1% من المشاركين الذين أعربوا عن عدم موافقتهم على أن مستوى الأمن السيبراني في المؤسسات الحكومية يلي الاحتياجات الحالية إلى وجود فجوة ملحوظة في فعالية استراتيجيات الحماية المتبعة، مما يبرز القلق المتزايد بشأن قدرة هذه المؤسسات على التصدي للتهديدات السيبرانية المتطورة. تعكس هذه النسبة إحساساً بعدم الاطمئنان حيال الأمن السيبراني، وهو ما قد يُعزى إلى نقص في التحديثات الدورية للأنظمة والبرمجيات، بالإضافة إلى عدم كفاية التدريب والتوعية للعاملين في هذا المجال. هذه الفجوة تعني أن المؤسسات قد تكون عرضة للهجمات السيبرانية، مما يستدعي ضرورة إعادة تقييم شاملة لاستراتيجيات الحماية، بما في ذلك الاستثمار في تقنيات جديدة وتطوير المهارات الفنية. علاوة على ذلك، يمكن أن تؤثر هذه الحالة سلباً على ثقة المواطنين في المؤسسات الحكومية، مما يجعل من الضروري تعزيز الشفافية والاتصال الفعال مع الجمهور حول التدابير المتخذة لحماية المعلومات. باختصار، هذه النسبة تشير إلى حاجة ملحة لتطبيق استراتيجيات أمن سيبراني أكثر تطوراً وفعالية لضمان الحماية المستمرة للبيانات والمعلومات الحيوية.

مستوى الأمن السيبراني في المؤسسات يلبي الاحتياجات الحالية					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أوافق	62	17.7	17.7	17.7
	أوافق بشدة	77	21.9	21.9	39.6
	لا أوافق	81	23.1	23.1	62.7
	لا أوافق بشدة	56	16.0	16.0	78.6
	لا أوافق ولا أرفض	75	21.4	21.4	100.0
	Total	351	100.0	100.0	

جدول 14: الوصف الاحصائي لمستوى الأمن السيبراني في المؤسسات يلبي الاحتياجات الحالية.



رسم توضيحي 14: التمثيل البياني لمستوى الأمن السيبراني في المؤسسات يلبي الاحتياجات الحالية

14. تقييم المؤسسات أداء مزودي خدمات الأمن السيبراني بشكل دوري.

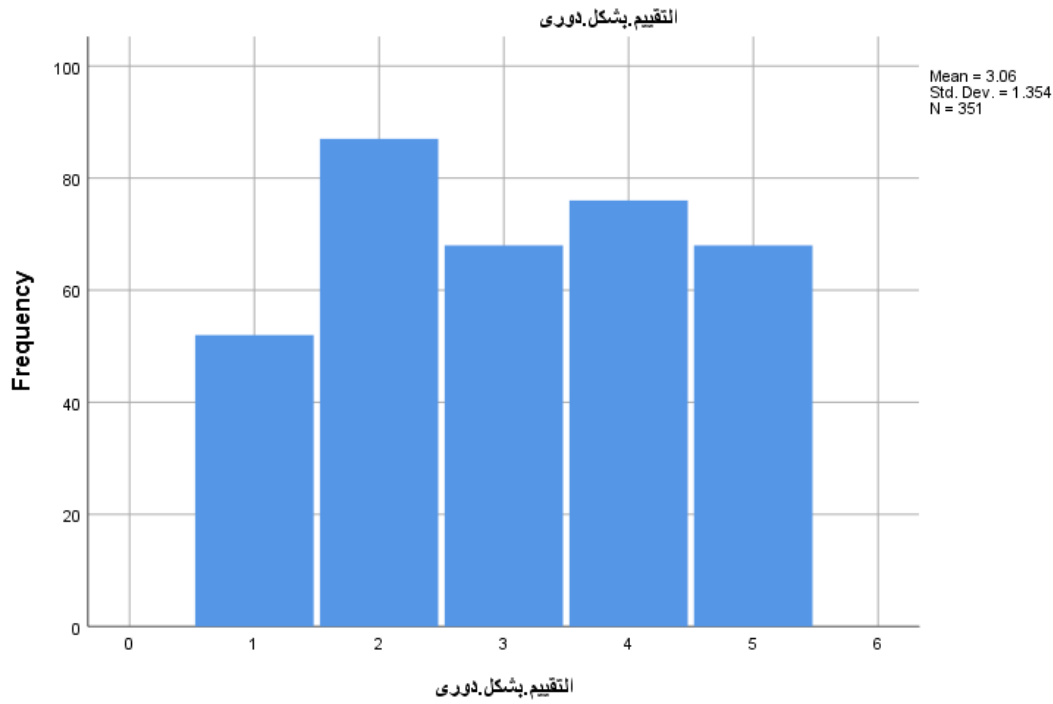
تشير نسبة 24.8% من المشاركين الذين أبدوا موافقتهم بشدة على أن المؤسسات الحكومية تقوم بتقييم أداء مزودي خدمات الأمن السيبراني بشكل دوري إلى إدراك مهم لأهمية المراجعة المستمرة لمستوى الخدمة المقدمة في هذا المجال الحساس. يُظهر هذا التأكيد التزام المؤسسات بالتحسين المستمر للأنظمة الأمنية وتعزيز فعالية استراتيجيات الحماية. إن تقييم أداء مزودي الخدمات يعد من العناصر الأساسية لضمان فعالية الإجراءات المتبعة في مواجهة التهديدات السيبرانية المتطورة، حيث يسمح للمؤسسات بتحديد نقاط القوة والضعف في الأنظمة المعتمدة، وتطبيق التغييرات الضرورية لتحسين الأداء.

تساهم هذه الممارسة أيضًا في تعزيز الشفافية والمساءلة، مما يعزز الثقة بين المؤسسات الحكومية والمواطنين. في عالم يتسم بتزايد الهجمات السيبرانية، فإن الاستناد إلى تقييم دوري يُعتبر أداة فعالة لتعزيز الأمن السيبراني، مما يضمن حماية البيانات الحساسة ويعزز من قدرة المؤسسات على التصدي للتحديات الحالية والمستقبلية. بالإضافة إلى ذلك، فإن هذه السياسة تشجع على الابتكار والتطوير المستمر في مجال تقنيات الأمن السيبراني، مما يساهم في خلق بيئة عمل أكثر أمانًا وموثوقية. بشكل عام، تعكس هذه النسبة اتجاهًا إيجابيًا نحو تعزيز ثقافة الأمن السيبراني في المؤسسات الحكومية، مما يعد خطوة ضرورية نحو تحقيق مستويات أعلى من الأمان.

تقييم المؤسسات أداء مزودي خدمات الأمن السيبراني بشكل دوري					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أوافق	52	14.8	14.8	14.8
	أوافق بشدة	87	24.8	24.8	39.6
	لا أوافق	68	19.4	19.4	59.0
	لا أوافق بشدة	76	21.7	21.7	80.6

	لا أوافق ولا أرفض	68	19.4	19.4	100.0
	Total	351	100.0	100.0	

جدول 15: الوصف الاحصائي لتقييم المؤسسات أداء مزودي خدمات الأمن السيبراني بشكل دوري



رسم توضيحي 15: التمثيل البياني لتقييم المؤسسات أداء مزودي خدمات الأمن السيبراني بشكل دوري

15. توجد ثقافة مؤسسية تدعم الأمن السيبراني بين جميع الموظفين.

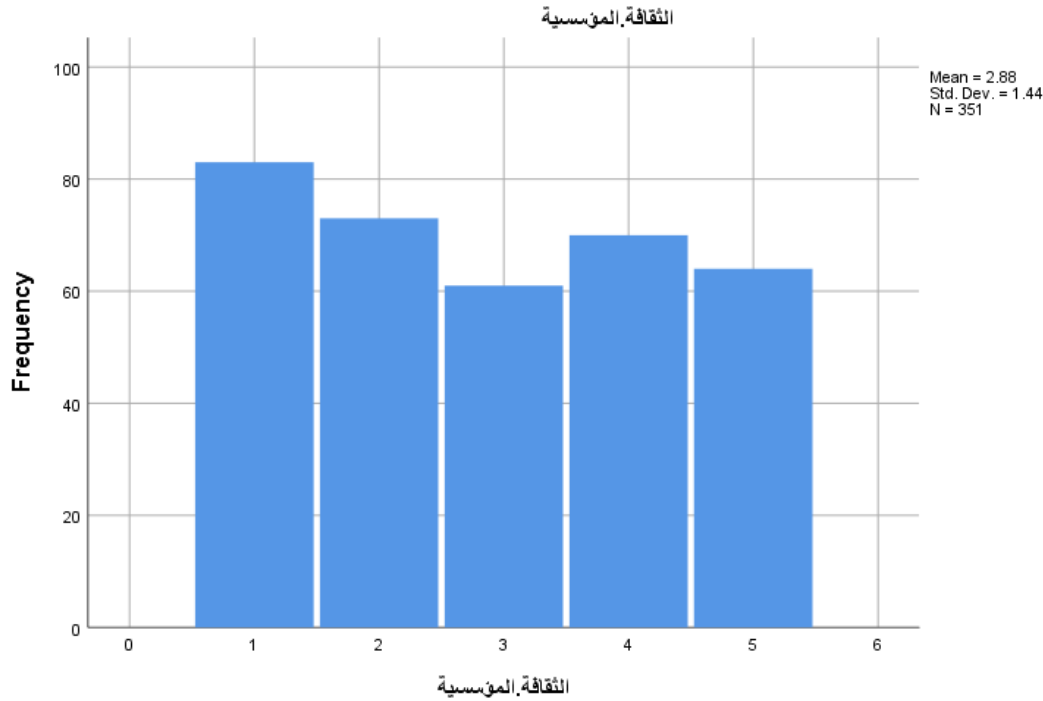
تشير نسبة 23.6% من المشاركين الذين أكدوا وجود ثقافة مؤسسية تدعم الأمن السيبراني بين جميع الموظفين إلى أهمية الوعي الجماعي في تعزيز الأمان السيبراني داخل المؤسسات الحكومية. يُظهر هذا التصريح فهمًا عميقًا للمسؤولية الجماعية تجاه حماية المعلومات والبيانات الحساسة، مما يعكس التزامًا من الإدارة العليا لتعزيز ثقافة الأمان بين الموظفين. وجود ثقافة مؤسسية تعزز من أهمية الأمن السيبراني يعني أن جميع الأفراد، من جميع المستويات، يتفاعلون

بفعالية مع ممارسات الأمان، ويشاركون في اتخاذ القرارات المرتبطة به، مما يقلل من احتمالات حدوث الأخطاء البشرية التي قد تؤدي إلى خروقات أمنية.

يمكن أن تساهم هذه الثقافة في تحسين القدرة على الاستجابة للتهديدات السيبرانية بشكل أسرع وأكثر فعالية، حيث سيكون لدى الموظفين المعرفة الكافية للتعرف على التهديدات المحتملة والتصرف وفقاً لذلك. إن تعزيز الوعي وتوفير التدريب المستمر في هذا المجال لا يسهم فقط في حماية المعلومات، بل يعزز أيضاً من الثقة بين الموظفين والإدارة، مما يخلق بيئة عمل أكثر أماناً وتعاوناً. بشكل عام، تعكس هذه النسبة اتجاهاً إيجابياً نحو تحقيق أهداف الأمن السيبراني في المؤسسات الحكومية، مما يعد خطوة مهمة نحو حماية البنية التحتية الحيوية للدولة وضمان استمرارية الخدمات الحكومية.

توجد ثقافة مؤسسية تدعم الأمن السيبراني بين جميع الموظفين					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أوافق	83	23.6	23.6	23.6
	أوافق بشدة	73	20.8	20.8	44.4
	لا أوافق	61	17.4	17.4	61.8
	لا أوافق بشدة	70	19.9	19.9	81.8
	لا أوافق ولا أرفض	64	18.2	18.2	100.0
	Total	351	100.0	100.0	

جدول 16: الوصف الاحصائي لوجود ثقافة مؤسسية تدعم الأمن السيبراني بين جميع الموظفين



رسم توضيحي 16: التمثيل البياني لوجود ثقافة مؤسسية تدعم الأمن السيبراني بين جميع الموظفين

16. تستخدم أدوات فعالة لرصد التهديدات السيبرانية في المؤسسات.

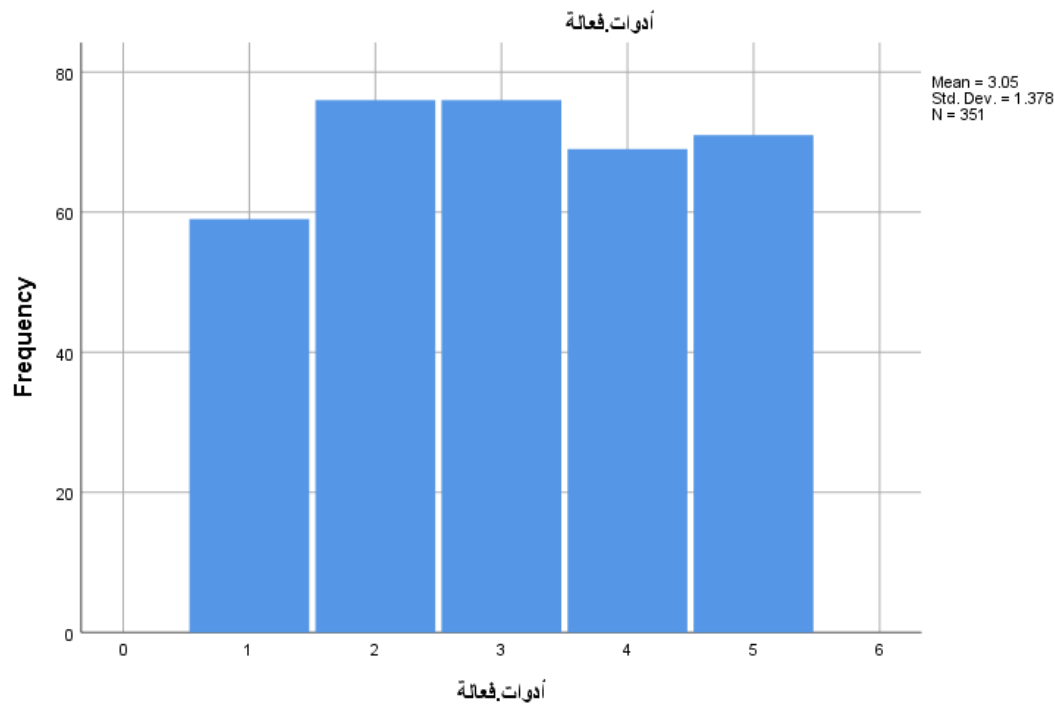
تشير نسبة 21.7% من المشاركين الذين أكدوا على استخدام أدوات فعالة لرصد التهديدات السيبرانية إلى وجود انقسام ملحوظ في وجهات النظر حول كفاءة هذه الأدوات داخل المؤسسات الحكومية. فالموافقة الشديدة من بعض المشاركين تدل على أن هناك أدوات وتكنولوجيا فعالة بالفعل تم اعتمادها، مما يعكس التزام المؤسسات بتعزيز قدراتها في مجال الأمن السيبراني. هذه الأدوات قد تشمل أنظمة الكشف عن التسلل، وبرامج تحليل البيانات الضخمة لرصد الأنماط غير المعتادة، وتقنيات الذكاء الاصطناعي التي تساعد في التعرف على التهديدات قبل حدوثها.

إن وجود نسبة من المشاركين الذين لم يوافقوا يعني أن هناك نقصاً في الوعي أو الثقة في فعالية هذه الأدوات، أو ربما عدم توافر هذه الأدوات بشكل كافٍ في بعض الأقسام أو المؤسسات. هذا الانقسام يُشير إلى الحاجة الماسة لتحسين التدريب وزيادة الوعي حول التقنيات المستخدمة، بالإضافة إلى ضرورة تقييم فعالية الأدوات المستخدمة في رصد التهديدات بشكل دوري. إذ أن تحسين كفاءة أدوات الرصد يساهم في تقليل المخاطر السيبرانية، ويعزز القدرة على الاستجابة السريعة للتهديدات، مما يوفر حماية أفضل للبيانات والمعلومات الحساسة. بالتالي، فإن تعزيز ثقافة الأمان

السيبراني وتوفير الأدوات والتدريب المناسبين يعتبران أساسيين لضمان فعالية استراتيجيات الحماية في المؤسسات الحكومية.

تستخدم أدوات فعالة لرصد التهديدات السيبرانية في المؤسسات					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أوافق	59	16.8	16.8	16.8
	أوافق بشدة	76	21.7	21.7	38.5
	لا أوافق	76	21.7	21.7	60.1
	لا أوافق بشدة	69	19.7	19.7	79.8
	لا أوافق ولا أرفض	71	20.2	20.2	100.0
	Total	351	100.0	100.0	

جدول 17: الوصف الاحصائي لأدوات فعالة لرصد التهديدات السيبرانية في المؤسسات



رسم توضيحي 17: التمثيل البياني لاستخدام أدوات فعالة لرصد التهديدات السيبرانية في المؤسسات

17. تعتبر الإجراءات المتخذة لحماية البيانات كافية في المؤسسات الحكومية.

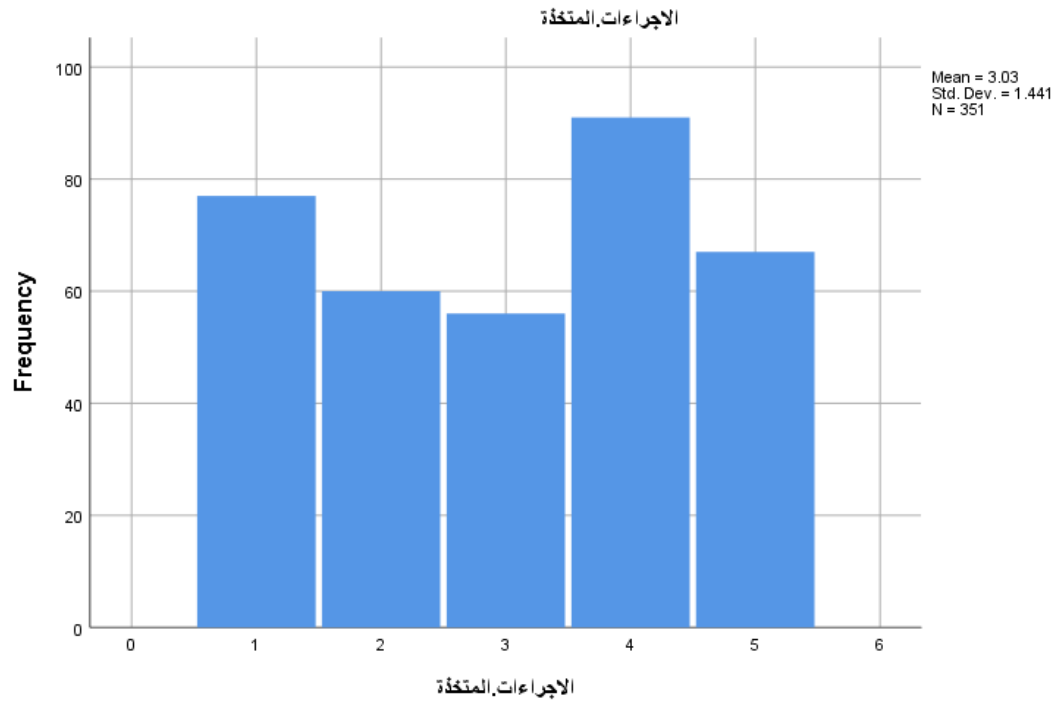
تشير نسبة 21.9% من المشاركين الذين أكدوا أن الإجراءات المتخذة لحماية البيانات تعتبر كافية في المؤسسات الحكومية إلى وجود مستوى من الثقة بين الموظفين في كفاءة التدابير الأمنية المتبعة. هذه النسبة تُظهر أن جزءاً من العاملين يشعر بالاطمئنان تجاه السياسات والأنظمة الأمنية المعمول بها، مما قد يعكس استثمارات حقيقية قامت بها المؤسسات في هذا المجال، مثل تحديث البرمجيات، وتطبيق تقنيات تشفير البيانات، وتطوير نظم مراقبة متقدمة.

إن هذه النسبة تعكس أيضاً احتمالية وجود فئة من الموظفين الذين قد يكون لديهم انطباعات متباينة حول فعالية هذه الإجراءات، مما يستدعي مزيداً من الاستقصاء والتحليل لفهم وجهات نظرهم. فالشعور بالرضا عن كفاية الإجراءات الأمنية لا يعني بالضرورة عدم وجود ثغرات أو مجالات تحتاج إلى تحسين. بالإضافة إلى ذلك، فإن التقييم الذاتي للإجراءات الأمنية يعد عملية ديناميكية تتطلب مراجعة دورية لضمان مواكبتها لأحدث التهديدات السيبرانية. لذا، يجب أن تعمل المؤسسات على تعزيز ثقافة الأمان السيبراني بين الموظفين، وتوفير التدريب اللازم، وتعزيز الشفافية حول

السياسات الأمنية المتبعة، لضمان أن تكون جميع الآراء والاحتياجات مُعالجة، وبالتالي تعزيز الحماية الفعالة للبيانات والمعلومات الحساسة.

تعتبر الإجراءات المتخذة لحماية البيانات كافية في المؤسسات الحكومية					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أوافق	77	21.9	21.9	21.9
	أوافق بشدة	60	17.1	17.1	39.0
	لا أوافق	56	16.0	16.0	55.0
	لا أوافق بشدة	91	25.9	25.9	80.9
	لا أوافق ولا أرفض	67	19.1	19.1	100.0
	Total	351	100.0	100.0	

جدول 18: الوصف الاحصائي لاعتبار الإجراءات المتخذة لحماية البيانات كافية في المؤسسات الحكومية



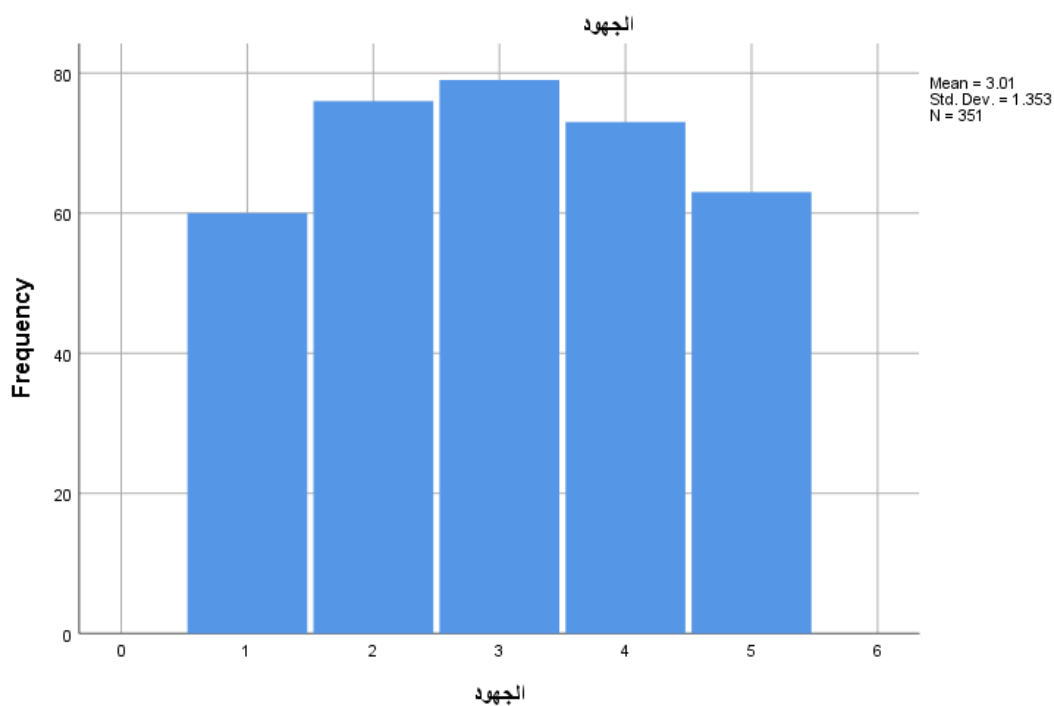
رسم توضيحي 18: التمثيل البياني لاعتبار الإجراءات المتخذة لحماية البيانات كافية في المؤسسات الحكومية

18. يشارك جميع الموظفين في جهود تعزيز الأمن السيبراني.

تشير نسبة 22.5% من المشاركين الذين أعربوا عن عدم موافقتهم على أن جميع الموظفين يشاركون في جهود تعزيز الأمن السيبراني إلى وجود فجوة ملحوظة في الوعي والمشاركة في هذا المجال الحيوي. هذا يعكس عدم التزام أو وعي كافٍ من قبل بعض الأفراد بشأن مسؤولياتهم تجاه حماية البيانات والمعلومات الرقمية، مما قد يؤثر سلبًا على فعالية الاستراتيجيات الأمنية المتبعة في المؤسسات الحكومية. فالأمن السيبراني يتطلب تعاونًا مشتركًا بين كافة الموظفين، حيث إن أي ضعف في هذا الجانب يمكن أن يؤدي إلى تعرض المؤسسة لتهديدات قد تكون مدمرة. لذا، من الضروري أن تعزز المؤسسات من برامج التوعية والتدريب المتعلقة بالأمن السيبراني، من خلال تنظيم ورش عمل ودورات تدريبية تفاعلية تشرح أهمية المشاركة الفردية في حماية المعلومات، وكيفية الإبلاغ عن أي سلوكيات مشبوهة. كما يجب أن تُعزز ثقافة المسؤولية المشتركة من خلال وضع سياسات واضحة تحدد أدوار الجميع في هذا السياق، مما يساعد على تعزيز الالتزام الجماعي ويساهم في خلق بيئة عمل أكثر أمانًا. وبذلك، فإن تحسين مستوى المشاركة من قبل جميع الموظفين في جهود الأمن السيبراني سيعزز من قدرة المؤسسات على مواجهة التحديات والتهديدات السيبرانية بفعالية أكبر.

يشارك جميع الموظفين في جهود تعزيز الأمن السيبراني.					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أوافق	60	17.1	17.1	17.1
	أوافق بشدة	76	21.7	21.7	38.7
	لا أوافق	79	22.5	22.5	61.3
	لا أوافق بشدة	73	20.8	20.8	82.1
	لا أوافق ولا أرفض	63	17.9	17.9	100.0
	Total	351	100.0	100.0	

جدول 19: الوصف الاحصائي لمشاركة جميع الموظفين في جهود تعزيز الأمن السيبراني.



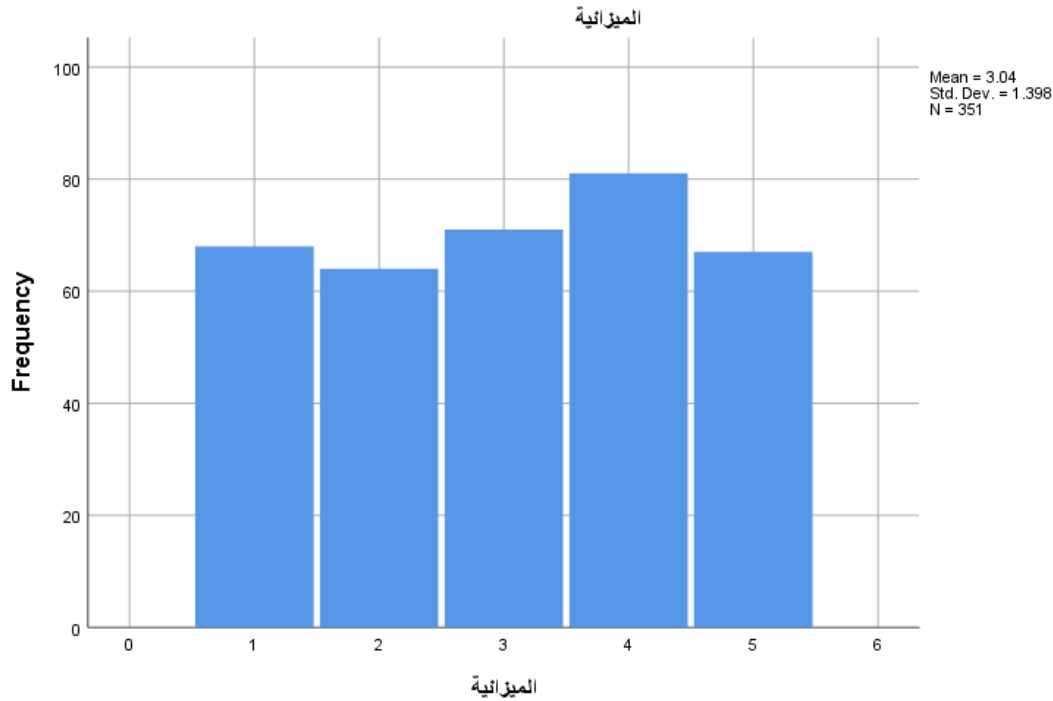
رسم توضيحي 19: التمثيل البياني لمشاركة جميع الموظفين في جهود تعزيز الأمن السيبراني

19. تدعم الميزانية المخصصة للأمن السيبراني في المؤسسات الحكومية.

تشير نسبة 23.1% من المشاركين الذين أبدوا عدم موافقتهم بشدة على أن الميزانية المخصصة للأمن السيبراني في المؤسسات الحكومية تدعم الجهود المبذولة في هذا المجال، إلى وجود قلق ملحوظ بشأن التوجهات المالية تجاه حماية البيانات والأنظمة. هذه النتيجة تعكس عدم رضا المشاركين عن مستوى الدعم المالي المخصص لأمن المعلومات، مما قد يعكس غياب التقدير الكافي لأهمية الأمن السيبراني في مواجهة التهديدات المتزايدة. يمكن أن تؤدي هذه الحالة إلى ضعف في القدرات الدفاعية للمؤسسات، حيث أن ضعف الميزانية يعني نقصاً في الموارد اللازمة لتوظيف تقنيات حديثة، وتدريب الموظفين، وتنفيذ استراتيجيات شاملة للحماية. لذا، من الضروري أن تعيد المؤسسات الحكومية تقييم استراتيجياتها المالية لضمان توفير دعم كافٍ للأمن السيبراني، مما يعزز من قدرة هذه المؤسسات على مواجهة التحديات الرقمية المستمرة وتحسين الثقة العامة في أنظمتها.

تدعم الميزانية المخصصة للأمن السيبراني في المؤسسات الحكومية.					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أوافق	68	19.4	19.4	19.4
	أوافق بشدة	64	18.2	18.2	37.6
	لا أوافق	71	20.2	20.2	57.8
	لا أوافق بشدة	81	23.1	23.1	80.9
	لا أوافق ولا أرفض	67	19.1	19.1	100.0
	Total	351	100.0	100.0	

جدول 20: الوصف الاحصائي لدعم الميزانية المخصصة للأمن السيبراني في المؤسسات الحكومية.



رسم توضيحي 20: التمثيل البياني لدعم الميزانية المخصصة للأمن السيبراني في المؤسسات الحكومية

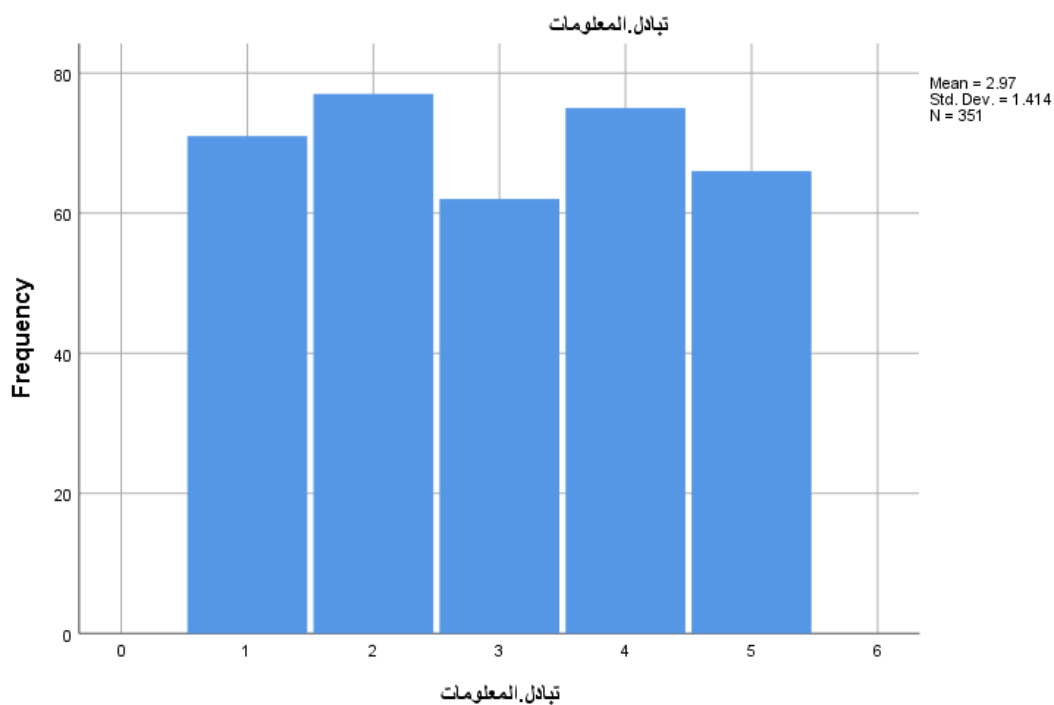
20. توجد آليات لتبادل المعلومات حول التهديدات السيبرانية بين المؤسسات.

تشير نسبة 21.9% من المشاركين الذين أبدوا موافقتهم بشدة على وجود آليات لتبادل المعلومات حول التهديدات السيبرانية بين المؤسسات إلى وجود وعي متزايد بأهمية التعاون والتنسيق في مجال الأمن السيبراني. هذه النسبة تعكس إيمان المشاركين بأن التعاون بين المؤسسات يمكن أن يسهم بشكل كبير في تحسين فعالية الاستجابة للتهديدات، حيث يُعتبر تبادل المعلومات أداة حيوية لرصد التهديدات المتزايدة ومشاركتها بين مختلف الجهات. إن وجود آليات فعالة لتبادل المعلومات يساهم في تعزيز قدرة المؤسسات على التعرف المبكر على التهديدات السيبرانية، مما يسمح باتخاذ إجراءات استباقية لتقليل الأضرار المحتملة. بالإضافة إلى ذلك، يمكن أن يؤدي هذا التعاون إلى تطوير استراتيجيات أمان موحدة، وتبادل المعرفة والخبرات، مما يعزز من كفاءة الحماية السيبرانية. بالتالي، يُظهر هذا التوجه أهمية الاستثمارات في تطوير وتعزيز هذه الآليات لضمان تحقيق مستوى أعلى من الأمان والاستجابة الفعالة للتحديات السيبرانية.

توجد آليات لتبادل المعلومات حول التهديدات السيبرانية بين المؤسسات.

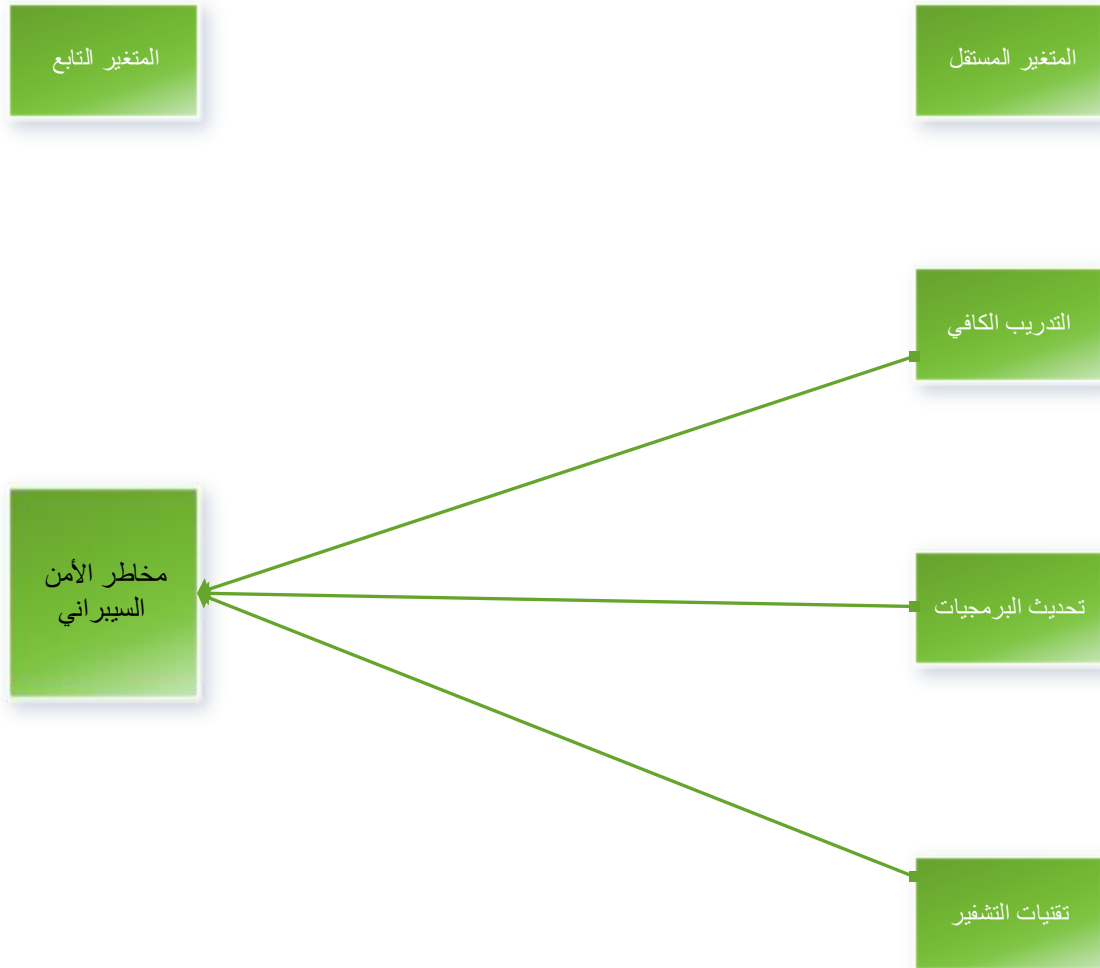
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أوافق	71	20.2	20.2	20.2
	أوافق بشدة	77	21.9	21.9	42.2
	لا أوافق	62	17.7	17.7	59.8
	لا أوافق بشدة	75	21.4	21.4	81.2
	لا أوافق ولا أرفض	66	18.8	18.8	100.0
	Total	351	100.0	100.0	

جدول 21: الوصف الاحصائي لوجود آليات لتبادل المعلومات حول التهديدات السيبرانية بين المؤسسات.



رسم توضيحي 21: التمثيل البياني لوجود آليات لتبادل المعلومات حول التهديدات السيبرانية بين المؤسسات

• متغيرات الدراسة



رسم توضيحي 22: متغيرات الدراسة التابعة والمستقلة

• دور التدريب الكافي في تقليل المخاطر السيبرانية بالمؤسسات الحكومية بالمملكة العربية السعودية

يعتبر التدريب الكافي للموظفين في المؤسسات الحكومية أحد العوامل الأساسية في تقليل المخاطر السيبرانية. يتزايد الاعتماد على التكنولوجيا والأنظمة الرقمية في الأعمال الحكومية، مما يجعلها عرضة للتهديدات السيبرانية المتنوعة. من خلال توفير برامج تدريبية شاملة، يتمكن الموظفون من التعرف على أساليب الهجوم السيبراني المختلفة، والتقنيات الحديثة المستخدمة في حماية البيانات. التدريب لا يقتصر فقط على المعرفة النظرية، بل يشمل أيضاً تطبيقات عملية تساهم في تعزيز الوعي السيبراني بين الموظفين، مما يمكنهم من اتخاذ خطوات استباقية للحماية.

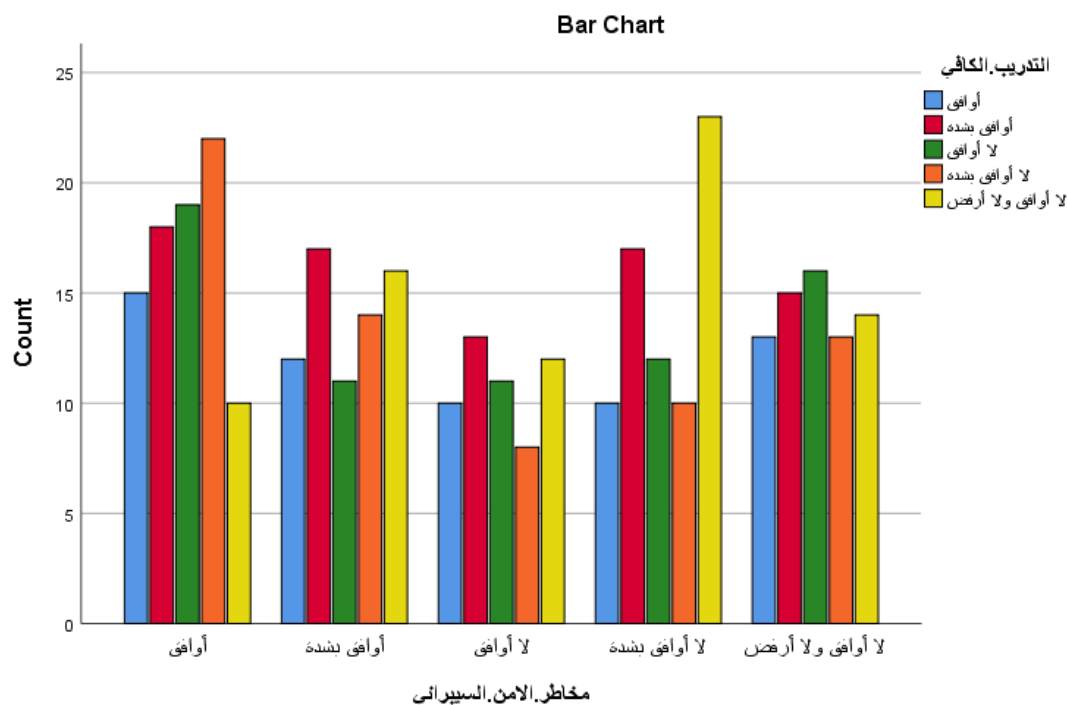
يعزز التدريب من قدرة الموظفين على الاستجابة لحالات الطوارئ. عندما يتمكن الموظفون من التعرف على التهديدات والاستجابة لها بسرعة وكفاءة، فإن ذلك يقلل من الأثر المحتمل للاختراقات السيبرانية. بجانب ذلك، يساهم التدريب المستمر في تطوير ثقافة أمنية داخل المؤسسة، حيث يشعر الموظفون بالمسؤولية تجاه حماية المعلومات. هذا التوجه الجماعي نحو الأمن السيبراني يعزز من قدرة المؤسسات الحكومية على التصدي للمخاطر ويقلل من احتمالية حدوث خروقات قد تؤثر على سلامة البيانات والخدمات المقدمة للمواطنين (Khando، 2021).

نتائج اختبارات كاي-تربيع (Chi-Square Tests) وجود علاقة غير دالة إحصائياً بين مستوى التدريب الكافي والوعي الأمني لدى الموظفين، حيث أظهرت القيم الناتجة، بما في ذلك قيمة Pearson Chi-Square التي بلغت 13.720 مع درجات حرية df تساوي 3، وأهمية دالة (Asymptotic Significance) تساوي 0.620، أن هناك نقصاً في الإشارة إلى وجود تأثير كبير للتدريب على تقليل المخاطر السيبرانية.

هذا يدل على أن الموظفين في المؤسسات الحكومية، بالرغم من تلقّيهم التدريب، قد لا يشعرون بالتغيير الفعلي في مستوى الأمان السيبراني، مما يعكس أن التدريب لوحده قد لا يكون كافياً إذا لم يترافق مع تطبيقات عملية أو تقنيات حديثة تساهم في تعزيز الثقافة الأمنية. بالإضافة إلى ذلك، قد تشير هذه النتائج إلى أن التركيز ينبغي أن يكون على تحسين جودة التدريب وتطبيقه بشكل فعال، لضمان تحقيق الفائدة المرجوة منه في حماية البيانات وتقليل المخاطر المحتملة. لذا، يُعتبر تحسين أساليب التدريب وتوفير الموارد اللازمة لتعزيز الوعي الأمني جزءاً أساسياً من الاستراتيجيات التي ينبغي أن تتبناها المؤسسات الحكومية، لضمان أن الموظفين ليسوا فقط مدربين، بل أيضاً قادرين على التعامل مع التهديدات السيبرانية بفعالية.

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	13.720 ^a	3	.620
Likelihood Ratio	13.870	3	.608
Linear-by-Linear Association	.495	1	.482
N of Valid Cases	351		
a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 9.23.			

جدول 22: اختبار كاي اسكوير لدور التدريب الكافي في تقليل المخاطر السيبرانية بالمؤسسات الحكومية بالمملكة العربية السعودية



رسم توضيحي 23: المقاييس المتماثلة في تحليل الجداول المتقاطعة لدور التدريب الكافي في تقليل المخاطر السيبرانية بالمؤسسات الحكومية بالمملكة العربية السعودية

• دور تحديث البرمجيات في تقليل المخاطر السيبرانية بالمؤسسات الحكومية بالمملكة العربية السعودية

يعتبر تحديث البرمجيات من العناصر الأساسية في استراتيجيات الأمن السيبراني بالمؤسسات الحكومية، حيث يساهم بشكل كبير في تقليل المخاطر المرتبطة بالثغرات الأمنية. تتطور التهديدات السيبرانية باستمرار، مما يجعل الأنظمة والبرمجيات القديمة عرضة للاختراقات. من خلال التحديثات الدورية، يتم تصحيح الثغرات الأمنية التي قد يستغلها المهاجمون، مما يعزز من مستوى الأمان ويقلل من فرص التعرض للهجمات.

تتضمن التحديثات عادةً تحسينات في الأداء والوظائف، مما يساهم في تعزيز كفاءة الأنظمة. هذه التحسينات ليست فقط تقنية، بل تشمل أيضاً تحسين آليات التشفير وحماية البيانات، مما يعزز من قدرة المؤسسات على حماية المعلومات الحساسة. من خلال الالتزام بعمليات تحديث منتظمة، يمكن للمؤسسات الحكومية ضمان أن أنظمتها تعمل بأعلى معايير الأمان، مما يساهم في بناء ثقة المستخدمين ويعزز من الاستقرار المؤسسي (tealtech، 2024).

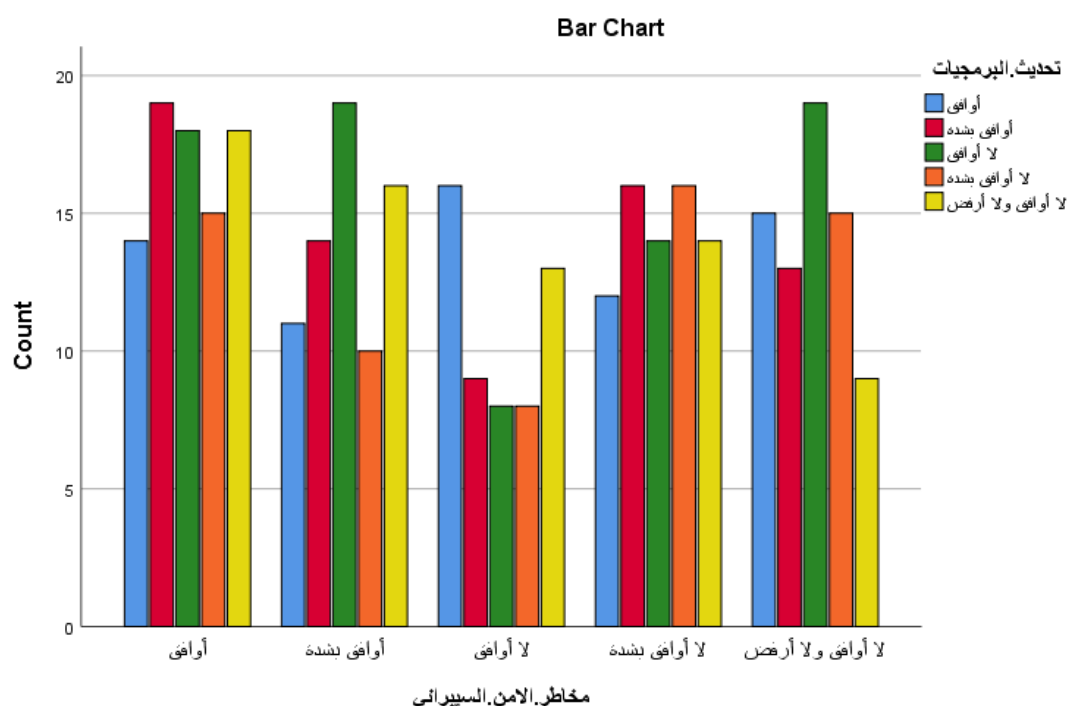
تعكس نتائج اختبارات كاي-تربيع (Chi-Square Tests) عدم وجود علاقة دالة إحصائية بين تحديث البرمجيات وتقليل المخاطر السيبرانية، حيث أظهرت قيمة Pearson Chi-Square البالغة 12.642 مع درجات حرية df تساوي 4، وأهمية دالة (Asymptotic Significance) التي تساوي 0.699، أن تحديث البرمجيات لا يبدو أنه يساهم بشكل ملحوظ في تعزيز الأمان السيبراني بالمؤسسات الحكومية.

هذا يشير إلى أن المؤسسات، رغم أنها قد تقوم بتحديث البرمجيات، إلا أن هذه العملية وحدها لا تكفي لتقليل المخاطر، حيث قد تكون هناك عوامل أخرى تؤثر في فعالية الأمن السيبراني، مثل طريقة تطبيق التحديثات، أو توفر التدريب المناسب للموظفين، أو حتى مستوى التوعية بالمخاطر. لذلك، من الضروري أن تكون استراتيجيات تحديث البرمجيات جزءاً من إطار شامل للأمن السيبراني يتضمن تدريباً مستمراً ورفع مستوى الوعي بين الموظفين، لضمان أن التحديثات لا تؤدي فقط إلى تصحيح الثغرات، بل أيضاً تدعم بيئة عمل آمنة تتسم بالاستجابة السريعة والفعالة للتهديدات السيبرانية.

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	12.642 ^a	4	.699
Likelihood Ratio	12.654	4	.698
Linear-by-Linear Association	.611	1	.434
N of Valid Cases	351		
a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 9.85.			

جدول 23: اختبار كاي اسكوير لدور تحديث البرمجيات في تقليل المخاطر السيبرانية بالمؤسسات الحكومية بالمملكة العربية السعودية.



رسم توضيحي 24: المقاييس المتمثلة في تحليل الجداول المتقاطعة لدور تحديث البرمجيات في تقليل المخاطر السيبرانية بالمؤسسات الحكومية بالمملكة العربية السعودية

• دور تقنيات التشفير في تقليل المخاطر السيبرانية بالمؤسسات الحكومية بالمملكة العربية السعودية

تعتبر تقنيات التشفير واحدة من الركائز الأساسية في حماية البيانات والمعلومات الحساسة بالمؤسسات الحكومية، حيث تسهم بشكل فعال في تقليل المخاطر السيبرانية. من خلال تحويل البيانات إلى صيغ غير قابلة للقراءة إلا للأشخاص المخولين، تضمن هذه التقنيات سرية المعلومات وتمنع الوصول غير المصرح به. هذا الأمر مهم بشكل خاص في السياقات الحكومية حيث تحتوي المعلومات على تفاصيل حساسة قد تؤثر على الأمن القومي أو خصوصية الأفراد.

عند تطبيق تقنيات التشفير بشكل فعال، يُمكن للمؤسسات الحكومية حماية البيانات أثناء نقلها وتخزينها، مما يحد من خطر التسريبات أو الاختراقات التي قد تحدث نتيجة الهجمات السيبرانية. علاوة على ذلك، تُسهم تقنيات التشفير في تعزيز ثقة المواطنين والمستخدمين في الحكومة، حيث يشعر الأفراد بالأمان بشأن بياناتهم الشخصية، مما يعزز من علاقات الثقة بين الحكومة والمواطنين (Staff, 2024).

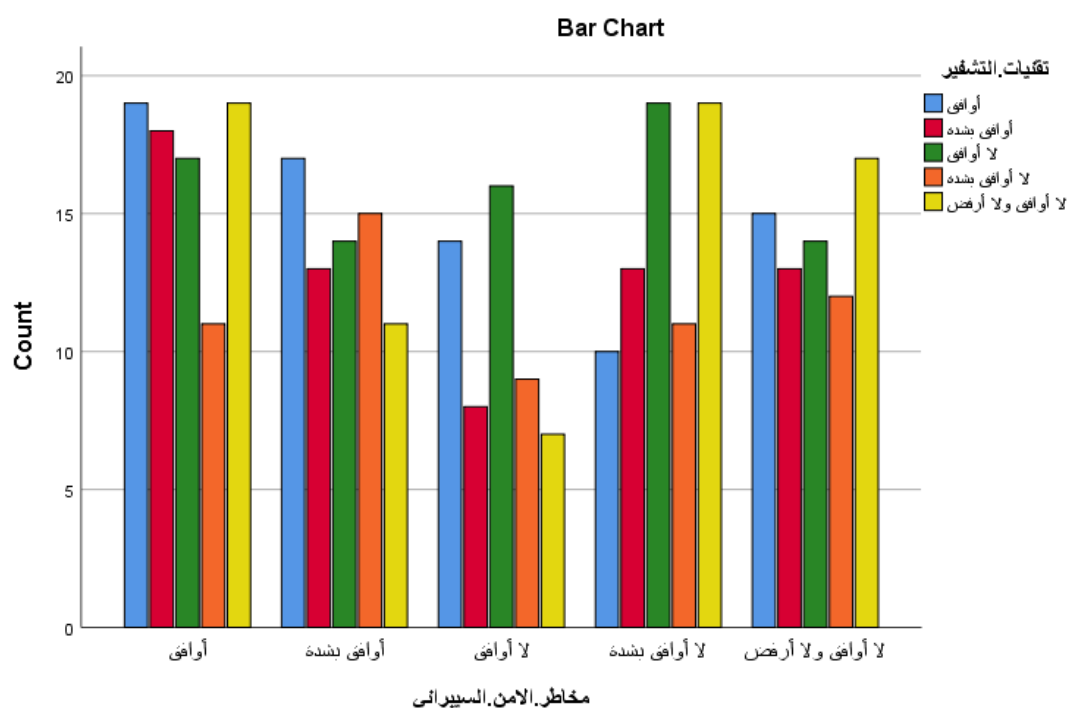
تشير نتائج اختبارات كاي-تربيع (Chi-Square Tests) إلى عدم وجود دلالة إحصائية قوية تربط بين استخدام تقنيات التشفير وتقليل المخاطر السيبرانية. حيث أظهرت قيمة Pearson Chi-Square التي بلغت 11.546 مع درجات حرية df تساوي 4، وأهمية دالة (Asymptotic Significance) التي تساوي 0.775، مما يعني أن هناك عدم ارتباط واضح بين استخدام تقنيات التشفير وتخفيف المخاطر السيبرانية في المؤسسات.

هذا يشير إلى أن مجرد اعتماد تقنيات التشفير لا يكفي بحد ذاته لخفض المخاطر بشكل فعال. يمكن أن يكون هناك عوامل أخرى مثل كفاءة تكامل هذه التقنيات ضمن استراتيجية الأمان الشاملة، ومدى التوعية والفهم لدى الموظفين حول أهمية التشفير وكيفية استخدامه بشكل صحيح. لذلك، من المهم أن تتبنى المؤسسات الحكومية استراتيجيات متعددة الطبقات تعزز من استخدام تقنيات التشفير، بالإضافة إلى التدريب والتوعية لضمان تحقيق أقصى استفادة من هذه التقنيات في حماية البيانات الحساسة وتعزيز أمان المعلومات.

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)

Pearson Chi-Square	11.546 ^a	4	.775
Likelihood Ratio	11.881	4	.752
Linear-by-Linear Association	1.319	1	.251
N of Valid Cases	351		
a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 8.92.			

جدول 24: اختبار كاي اسكوير لدور تقنيات التشفير في تقليل المخاطر السيبرانية بالمؤسسات الحكومية بالمملكة العربية السعودية



رسم توضيحي 25: المقاييس المتماثلة في تحليل الجداول المتقاطعة لدور تقنيات التشفير في تقليل المخاطر السيبرانية بالمؤسسات الحكومية بالمملكة العربية السعودية

• تحليل المصدقية والموثوقية

تشير نتائج تحليل المصدقية والموثوقية إلى أن أداة القياس المستخدمة في الدراسة تتمتع بمستوى مقبول من الموثوقية، حيث بلغ معامل ألفا كرونباخ 0.718. يُعتبر هذا الرقم مناسباً في الأبحاث الاجتماعية، حيث يُظهر أن الأداة قادرة على قياس المفاهيم بشكل موحد ودقيق. إن وجود 351 حالة صالحة دون أي حالات مستبعدة يدل على أن العينة كانت كاملة ومتاحة للتحليل، مما يعزز من موثوقية النتائج المستخلصة.

إن معامل ألفا القائم على العناصر القياسية (0.723) يشير إلى أن العناصر المستخدمة في الدراسة تعمل بشكل جيد معاً، مما يعزز من قدرة الأداة على قياس مفهوم الأمن السيبراني بفاعلية. هذا الأمر يدعم الافتراض بأن النتائج المستخلصة من هذه الدراسة يمكن الاعتماد عليها بشكل كبير، مما يوفر أساساً قوياً لاستنتاجات الدراسة وتوصياتها المتعلقة بمخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية.

Case Processing Summary			
		N	%
Cases	Valid	351	100.0
	Excluded ^a	0	.0
	Total	351	100.0
a. Listwise deletion based on all variables in the procedure.			

جدول 25: ملخص انجاز القضية.

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.718	.723	20

جدول 26: احصائيات الموثوقية.

التوصيات

تشمل توصيات الدراسة عدة جوانب رئيسية تهدف إلى تحسين استراتيجيات الحماية السيبرانية في المؤسسات الحكومية بالمملكة العربية السعودية، كما يلي:

- أظهرت الدراسة أن هناك ضعفًا في تدريب الموظفين على التعامل مع التهديدات السيبرانية. لذا، توصي الدراسة بضرورة تطوير برامج تدريبية مكثفة ومتخصصة في الأمن السيبراني تشمل جميع المستويات الإدارية. هذه البرامج يجب أن تشمل تدريب الموظفين على كيفية التعرف على الهجمات السيبرانية، مثل التصيد الاحتيالي، والهجمات عبر البريد الإلكتروني، وتجنب الأخطاء البشرية التي قد تؤدي إلى خرق أمني.
- نظرا لأن التهديدات السيبرانية تتطور بشكل مستمر، فإن التحديث الدوري للأنظمة والتطبيقات المستخدمة في المؤسسات الحكومية يُعد أمرًا ضروريًا. توصي الدراسة بتطبيق آلية صارمة لتحديث البرمجيات بشكل مستمر، بما في ذلك تصحيحات الأمان التلقائية التي تقلل من احتمالية استغلال الثغرات الموجودة في الأنظمة القديمة.
- تحتاج المؤسسات الحكومية إلى خطط استجابة فعالة للحوادث السيبرانية تتكيف مع نوعية التهديدات الجديدة. توصي الدراسة بتطوير خطط استجابة مرنة تتيح للمؤسسات التعامل مع مختلف أنواع الهجمات بشكل فوري وفعال. يتطلب ذلك اختبار الخطط بشكل دوري من خلال محاكاة حقيقية للهجمات السيبرانية.
- توصي الدراسة بتعزيز التعاون بين مختلف المؤسسات الحكومية في مجال تبادل المعلومات حول التهديدات السيبرانية المشتركة. يمكن تحقيق ذلك من خلال إنشاء شبكة مشتركة للتنسيق بين الجهات الحكومية، بالإضافة إلى تنظيم ورش عمل ومؤتمرات دورية لمناقشة التحديات التي تواجهها كل مؤسسة والحلول الممكنة.
- بالرغم من استخدام المؤسسات الحكومية لتقنيات التشفير والجدران النارية، فإن الدراسة توصي بالاستثمار في تقنيات الأمان المتقدمة مثل الذكاء الاصطناعي والتعلم الآلي للكشف المبكر عن الهجمات. هذه التقنيات يمكن أن تعزز من قدرة الأنظمة على اكتشاف التهديدات السيبرانية في مراحلها الأولية قبل أن تتسبب في أضرار كبيرة.
- توصي الدراسة بإعادة النظر في التشريعات الحالية المتعلقة بالأمن السيبراني في المملكة. يجب أن تتماشى القوانين مع التطورات التكنولوجية المستمرة لضمان تغطية جميع التهديدات السيبرانية الناشئة.

- من الضروري تشجيع الشركات الخاصة العاملة في مجال الأمن السيبراني على تطوير حلول جديدة تتناسب مع احتياجات المؤسسات الحكومية. يمكن تحقيق ذلك من خلال توفير بيئة تنظيمية داعمة للشركات الصغيرة والمتوسطة المتخصصة في هذا المجال، وتشجيع التعاون بين القطاعين العام والخاص.

المراجع

- Admass, W. S. (2024). Cyber security: State of the art, challenges and future directions☆. Retrieved from <https://www.sciencedirect.com/science/article/pii/S2772918423000188>
- Akter, S. (2022). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. Retrieved from <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9345286/>
- Alhakami, W. (2024). Enhancing Cybersecurity Competency in the Kingdom of Saudi Arabia: A Fuzzy Decision-Making Approach. Retrieved from <https://openurl.ebsco.com/EPDB%3Agcd%3A16%3A19342416/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A178454206&crl=c>
- Alhalafi, N. (2021). Cybersecurity Policy Framework in Saudi Arabia: Literature Review. Retrieved from <https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.736874/full>
- Alhejaili, M. O. (2024). Securing the Kingdom's e-commerce frontier: Evaluation of Saudi Arabia's cybersecurity legal frameworks. Retrieved from https://www.researchgate.net/publication/380942605_Securing_the_Kingdom's_e-commerce_frontier_Evaluation_of_Saudi_Arabia's_cybersecurity_legal_frameworks
- Almomani, I. (2021). Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia. Retrieved from <https://peerj.com/articles/cs-703/>
- Alrubaiq, A. (2021). Retrieved from <https://www.mdpi.com/2624-800X/1/2/17>
- Alshammari, A. (2023). A Novel Security Framework to Mitigate and Avoid Unexpected Security Threats in Saudi Arabia. 13(4). Retrieved from <https://www.etasr.com/index.php/ETASR/article/view/6091>
- Borky, J. M. (2018). Protecting Information with Cybersecurity. Retrieved from <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7122347/>
- Cremer, F. (2022). Cyber risk and cybersecurity: a systematic review of data availability. Retrieved from <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8853293/>
- Dawodu, S. O. (2023). CYBERSECURITY RISK ASSESSMENT IN BANKING: METHODOLOGIES AND BEST PRACTICES. Retrieved from https://www.researchgate.net/publication/376806023_CYBERSECURITY_RISK_ASSESSMENT_IN_BANKING_METHODOLOGIES_AND_BEST_PRACTICES
- Giannaros, A. (2023). Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions. Retrieved from <https://www.mdpi.com/2624-800X/3/3/25>
- Kaur, R. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Retrieved from <https://www.sciencedirect.com/science/article/pii/S1566253523001136>
- Khando, K. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. Retrieved from <https://www.sciencedirect.com/science/article/pii/S0167404821000912>

- Kure, H. (2021). An Assets Focus Risk Management Framework for Critical Infrastructure Cyber Security Risk Management. Retrieved from https://www.researchgate.net/publication/332969258_An_Assets_Focus_Risk_Management_Framework_for_Critical_Infrastructure_Cyber_Security_Risk_Management
- Li, Y. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Retrieved from <https://www.sciencedirect.com/science/article/pii/S2352484721007289>
- Lostri, E. (2022). A Shared Responsibility: Public-Private Cooperation for Cybersecurity. Retrieved from <https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity>
- Mishra, A. (2022). Attributes impacting cybersecurity policy development: An evidence from seven nations. Retrieved from <https://www.sciencedirect.com/science/article/pii/S0167404822002140>
- Obi, O. C. (2024). COMPREHENSIVE REVIEW ON CYBERSECURITY: MODERN THREATS AND ADVANCED DEFENSE STRATEGIES. Retrieved from https://www.researchgate.net/publication/377957344_COMPREHENSIVE_REVIEW_ON_CYBERSECURITY_MODERN_THREATS_AND_ADVANCED_DEFENSE_STRATEGIES
- Olabode, O. (2023). The Relevance Of Cybersecurity Awareness Training For Employees In Small and Medium Enterprises (SMEs). Retrieved from https://www.researchgate.net/publication/376538971_The_Relevance_Of_Cybersecurity_Awareness_Training_For_Employees_In_Small_and_Medium_Enterprises_SMEs
- Pryimenko, L. (2024). 5 Key Steps on How to Perform a Cybersecurity Risk Assessment. Retrieved from <https://www.ekransystem.com/en/blog/how-to-perform-a-cybersecurity-risk-assessment>
- Staff . (2024). Understanding the Role of Encryption in Protecting Data. Retrieved from <https://www.softwareseni.com/understanding-the-role-of-encryption-in-protecting-data/>
- tealtech. (2024). Why Software Updates Are Important for Cybersecurity. Retrieved from <https://tealtech.com/blog/why-software-updates-are-important/>

الملاحق

الاستبانة

- الاسئلة العامة

- العمر

- الجنس

- الدرجة

- أسئلة الاستبانة

- يعتبر الأمن السيبراني أولوية رئيسية في المؤسسات الحكومية.
- توفر المؤسسات الحكومية تدريباً كافياً للموظفين حول ممارسات الأمن السيبراني.
- توجد سياسات واضحة لمواجهة التهديدات السيبرانية في المؤسسات الحكومية.
- يتم تحديث البرمجيات والتطبيقات بشكل دوري لحماية البيانات الحساسة.
- تجرى تقييمات دورية للمخاطر السيبرانية في المؤسسات الحكومية.
- تُستخدم تقنيات التشفير لحماية البيانات الحساسة في المؤسسات.
- توجد خطط استجابة واضحة لحالات الطوارئ السيبرانية.
- يتم تشجيع الموظفين على الإبلاغ عن أي تهديدات تتعلق بالأمن السيبراني.
- تشجع المؤسسات الحكومية الابتكار في تقنيات الأمن السيبراني.
- مستوى الأمن السيبراني في المؤسسات يلبي الاحتياجات الحالية.
- تقيم المؤسسات أداء مزودي خدمات الأمن السيبراني بشكل دوري.
- توجد ثقافة مؤسسية تدعم الأمن السيبراني بين جميع الموظفين.
- تستخدم أدوات فعالة لرصد التهديدات السيبرانية في المؤسسات.
- تعتبر الإجراءات المتخذة لحماية البيانات كافية في المؤسسات الحكومية.
- يشارك جميع الموظفين في جهود تعزيز الأمن السيبراني.
- تدعم الميزانية المخصصة للأمن السيبراني في المؤسسات الحكومية.
- توجد آليات لتبادل المعلومات حول التهديدات السيبرانية بين المؤسسات.

<https://docs.google.com/forms/d/1AdxC5gFO6TgqnfbuaxrDcRXzvpDe43XsFpINCxZzfGY/edit>

Abstract

This study aims to assess cybersecurity risks in government institutions in the Kingdom of Saudi Arabia, with a focus on the protection and mitigation strategies used to address these risks. This study comes considering the rapid technological developments that make government institutions vulnerable to increasing cyber threats targeting digital infrastructure. The study used the descriptive analytical approach, as data was collected through questionnaires distributed to a sample of government employees specialized in the field of cybersecurity, in addition to conducting in-depth interviews with information security officials in some institutions. The results indicated that there are gaps in the implementation of some protection strategies, especially in the field of employee training and continuous updating of systems. The results also showed that government institutions rely heavily on technical solutions such as encryption systems and firewalls, but they need to enhance cooperation between government agencies and develop more comprehensive policies to mitigate risks. The study recommends the need to adopt cyber incident response plans that are more dynamic and adaptable to the development of threats, in addition to developing ongoing awareness programs to enhance employee awareness of the importance of cybersecurity.

Keywords: Cybersecurity, Government Institutions, Saudi Arabia, Protection Strategies, Risk Management, Risk Mitigation, Cyber Threats.

Midocean University

College of Management

Specialization in Risk Management



Title in English

**Cybersecurity Risk Assessment in Government Institutions in the Kingdom of Saudi Arabia
Protection and Mitigation Strategies**

Prepared by:

Madhawi Mohammad Al Mutairi

Supervised by:

Asma Abu Anza

Year: 2024