

إطار متكامل لإدارة مخاطر وتأمين البيانات الحساسة المتداولة عبر مزودي الخدمات من الأطراف الثالثة

إعداد الطالب/

فهد ابراهيم احمد المناع

252000840

إشراف/

د. الفصيل عبد الحميد

د. فايز جراد

العام الدراسي:

2026

فهرس المحتويات:

7	الفصل الأول
8	المقدمة:
9	-مشكلة الدراسة.
10	-أهمية الدراسة.
11	-أهداف الدراسة.
12	-تساؤلات الدراسة
13	-فروض الدراسة
14	-النظرية العلمية المتبعة لإعداد البحث
15	الفصل الثاني
15	الدراسات السابقة
16	-مقدمة
17	-الدراسات السابقة.
19	-الإطار النظري
21	الفصل الثالث
21	منهجية الدراسة
22	-مقدمة
23	-المنهجية وطرق البحث
24	-مجتمع البحث
25	-حدود البحث
26	الفصل الرابع
26	النتائج والتوصيات
27	-مقدمة
28	-تحليل البيانات
30	-النتائج
31	-التوصيات
32	المراجع
33	-المراجع العربية
34	-المراجع الأجنبية
35	الملاحق

36.....-الاستبانة

38..... Abstract الملخص

قائمة الجداول :

- جدول (1): مقارنة الدراسات السابقة
- جدول (2): منهجية البحث المعتمدة
- جدول (3): توزيع مجتمع البحث حسب التخصص
- جدول (4): حدود الدراسة
- جدول (5): مستوى الوعي بأمن المعلومات
- جدول (6): المخاطر المرتبطة بالأطراف الثالثة
- جدول (7): إجراءات حماية البيانات الحساسة
- جدول (8): أسئلة الاستبانة (الوعي الأمني)
- جدول (9): أسئلة الاستبانة (مخاطر الأطراف الثالثة)
- جدول (10): أسئلة الاستبانة (حماية البيانات)

المستخلص : Abstract

تهدف هذه الدراسة إلى تحليل المخاطر المرتبطة بحماية البيانات الحساسة عند تداولها عبر مزودي الخدمات من الأطراف الثالثة، وذلك في ظل التوسع الكبير في استخدام التقنيات الرقمية والخدمات السحابية داخل المؤسسات.

حيث أصبحت البيانات الحساسة تمثل أحد أهم الأصول الاستراتيجية التي تعتمد عليها المؤسسات في إدارة أعمالها واتخاذ قراراتها، الأمر الذي يجعل حمايتها من الاختراق أو التسريب ضرورة ملحة.

تتمثل مشكلة الدراسة في اعتماد العديد من المؤسسات على مزودي الخدمات الخارجيين دون وجود إطار واضح لإدارة المخاطر المرتبطة بهذا الاعتماد، مما يزيد من احتمالية تعرض البيانات الحساسة للتهديدات الأمنية. ومن هنا تسعى الدراسة إلى الإجابة عن السؤال الرئيس المتعلق بكيفية إدارة مخاطر وتأمين البيانات الحساسة المتداولة عبر الأطراف الثالثة بطريقة فعالة.

اعتمدت الدراسة على المنهج الوصفي التحليلي، حيث تم جمع البيانات من خلال الاستبانة الموجهة إلى عينة من العاملين في مجال تكنولوجيا المعلومات وأمن المعلومات داخل المؤسسات التي تعتمد على مزودي الخدمات الخارجيين. كما تم تحليل البيانات باستخدام مجموعة من الأساليب الإحصائية بهدف الوصول إلى نتائج دقيقة تدعم أهداف الدراسة.

وقد توصلت الدراسة إلى مجموعة من النتائج المهمة، من أبرزها أن التعامل مع الأطراف الثالثة يمثل أحد أهم مصادر المخاطر المرتبطة بأمن المعلومات، خاصة في ظل غياب السياسات الواضحة لإدارة هذه المخاطر. كما أظهرت النتائج أن استخدام التقنيات الحديثة مثل التشفير وأنظمة كشف التسلل يسهم بشكل كبير في تعزيز مستوى حماية البيانات الحساسة.

وأوصت الدراسة بضرورة تطوير إطار متكامل لإدارة مخاطر البيانات الحساسة، يشمل الجوانب التقنية والتنظيمية والبشرية، إضافة إلى ضرورة تعزيز مستوى الوعي الأمني داخل المؤسسات، وإجراء تقييم دوري لمستوى الأمان لدى مزودي الخدمات من الأطراف الثالثة.

وفي ضوء ما سبق، تؤكد الدراسة على أهمية تبني المؤسسات لاستراتيجيات شاملة لإدارة المخاطر الأمنية، بما يضمن حماية البيانات الحساسة وتحقيق مستوى عالٍ من الأمن السيبراني في بيئة الأعمال الرقمية.

الفصل الأول

المقدمة:

شهد العالم في السنوات الأخيرة تطوراً متسارعاً في مجال تكنولوجيا المعلومات والاتصالات، حيث أصبحت الأنظمة الرقمية جزءاً أساسياً من عمل المؤسسات في مختلف القطاعات. وقد أدى هذا التحول الرقمي إلى زيادة الاعتماد على البيانات كمورد أساسي في دعم العمليات التشغيلية واتخاذ القرارات الاستراتيجية. ولم تعد البيانات مجرد وسيلة مساعدة، بل أصبحت تمثل أحد أهم الأصول التي تمتلكها المؤسسات، خاصة البيانات الحساسة التي تتطلب مستوى عالياً من الحماية.

ومع التطور الكبير في استخدام التقنيات الحديثة مثل الحوسبة السحابية والأنظمة الموزعة، اتجهت المؤسسات إلى الاعتماد على مزودي الخدمات من الأطراف الثالثة لتقديم خدمات تقنية متعددة، مثل تخزين البيانات، وإدارة الأنظمة، وتحليل المعلومات. وعلى الرغم من الفوائد التي تقدمها هذه الخدمات، مثل تقليل التكاليف وزيادة الكفاءة التشغيلية، إلا أنها في المقابل تطرح مجموعة من التحديات المتعلقة بأمن المعلومات وحماية البيانات الحساسة.

إن نقل البيانات الحساسة إلى بيئات خارجية تديرها جهات أخرى يقلل من مستوى التحكم المباشر للمؤسسة على هذه البيانات، مما يزيد من احتمالية تعرضها لمخاطر الاختراق أو التسريب أو سوء الاستخدام. كما أن ضعف الرقابة أو غياب السياسات الواضحة لإدارة العلاقة مع الأطراف الثالثة قد يؤدي إلى حدوث ثغرات أمنية يمكن استغلالها من قبل المهاجمين.

وتكمن أهمية هذه الدراسة في تسليط الضوء على المخاطر المرتبطة بتداول البيانات الحساسة عبر مزودي الخدمات من الأطراف الثالثة، وتحليل العوامل التي تؤثر على مستوى أمن هذه البيانات، إضافة إلى تقديم إطار يساعد المؤسسات على إدارة هذه المخاطر بشكل أكثر فعالية.

-مشكلة الدراسة.

شهد العالم في السنوات الأخيرة تطوراً متسارعاً في مجال تكنولوجيا المعلومات والاتصالات، حيث أصبحت الأنظمة الرقمية جزءاً أساسياً من عمل المؤسسات في مختلف القطاعات. وقد أدى هذا التحول الرقمي إلى زيادة الاعتماد على البيانات كمورد أساسي في دعم العمليات التشغيلية واتخاذ القرارات الاستراتيجية. ولم تعد البيانات مجرد وسيلة مساعدة، بل أصبحت تمثل أحد أهم الأصول التي تمتلكها المؤسسات، خاصة البيانات الحساسة التي تتطلب مستوى عالياً من الحماية.

ومع التطور الكبير في استخدام التقنيات الحديثة مثل الحوسبة السحابية والأنظمة الموزعة، اتجهت المؤسسات إلى الاعتماد على مزودي الخدمات من الأطراف الثالثة لتقديم خدمات تقنية متعددة، مثل تخزين البيانات، وإدارة الأنظمة، وتحليل المعلومات. وعلى الرغم من الفوائد التي تقدمها هذه الخدمات، مثل تقليل التكاليف وزيادة الكفاءة التشغيلية، إلا أنها في المقابل تطرح مجموعة من التحديات المتعلقة بأمن المعلومات وحماية البيانات الحساسة.

إن نقل البيانات الحساسة إلى بيئات خارجية تديرها جهات أخرى يقلل من مستوى التحكم المباشر للمؤسسة على هذه البيانات، مما يزيد من احتمالية تعرضها لمخاطر الاختراق أو التسريب أو سوء الاستخدام. كما أن ضعف الرقابة أو غياب السياسات الواضحة لإدارة العلاقة مع الأطراف الثالثة قد يؤدي إلى حدوث ثغرات أمنية يمكن استغلالها من قبل المهاجمين.

وتكمن أهمية هذه الدراسة في تسليط الضوء على المخاطر المرتبطة بتداول البيانات الحساسة عبر مزودي الخدمات من الأطراف الثالثة، وتحليل العوامل التي تؤثر على مستوى أمن هذه البيانات، إضافة إلى تقديم إطار يساعد المؤسسات على إدارة هذه المخاطر بشكل أكثر فعالية.

-أهمية الدراسة.

الأهمية العلمية

- تسهم الدراسة في إثراء المعرفة العلمية في مجال أمن المعلومات وإدارة المخاطر.
- توضح المفاهيم المرتبطة بالبيانات الحساسة ومخاطر الأطراف الثالثة.
- تقدم إطاراً نظرياً يمكن أن يدعم الدراسات المستقبلية في هذا المجال.
- تساعد في تحليل الدراسات السابقة وتحديد الفجوات البحثية.

الأهمية العملية

- تساعد المؤسسات على فهم المخاطر المرتبطة بالتعامل مع الأطراف الثالثة.
- تقدم توصيات عملية لتعزيز حماية البيانات الحساسة.
- تسهم في تطوير السياسات الأمنية داخل المؤسسات.
- تساعد في تقليل احتمالية التعرض للاختراقات الأمنية.
- تعزز مستوى الوعي الأمني لدى العاملين في المؤسسات.

-أهداف الدراسة.

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف، من أبرزها:

- التعرف على مفهوم البيانات الحساسة وأهميتها.
- تحليل المخاطر المرتبطة بتداول البيانات عبر الأطراف الثالثة.
- دراسة دور مزودي الخدمات في إدارة البيانات.
- تحديد التحديات التي تواجه المؤسسات في حماية البيانات.
- اقتراح إطار متكامل لإدارة مخاطر البيانات الحساسة.

-تساؤلات الدراسة

السؤال الرئيس

كيف يمكن للمؤسسات إدارة مخاطر وتأمين البيانات الحساسة المتداولة عبر مزودي الخدمات من الأطراف الثالثة؟

الأسئلة الفرعية

- ما المقصود بالبيانات الحساسة؟
- ما أبرز المخاطر المرتبطة بالأطراف الثالثة؟
- ما العوامل التي تؤدي إلى تسريب البيانات؟
- ما مدى التزام مزودي الخدمات بالمعايير الأمنية؟
- ما الإجراءات التي يمكن اتخاذها لحماية البيانات؟

-فروض الدراسة

تستند الدراسة إلى مجموعة من الفروض التي سيتم اختبارها، ومن أبرزها:

1. توجد علاقة ذات دلالة إحصائية بين استخدام مزودي الخدمات من الأطراف الثالثة وزيادة مخاطر البيانات الحساسة.
2. توجد علاقة ذات دلالة إحصائية بين مستوى الوعي بأمن المعلومات داخل المؤسسة وتقليل مخاطر تسريب البيانات.
3. توجد علاقة ذات دلالة إحصائية بين تطبيق السياسات الأمنية وتقليل احتمالية الاختراق.
4. استخدام التقنيات الحديثة في الأمن السيبراني يساهم في تعزيز حماية البيانات الحساسة.

-النظرية العلمية المتبعة لإعداد البحث

تعتمد هذه الدراسة على مجموعة من النظريات العلمية المرتبطة بمجال أمن المعلومات وإدارة المخاطر، ومن أبرزها:

1. نظرية أمن المعلومات (Information Security Theory)

تركز هذه النظرية على حماية البيانات من التهديدات المختلفة من خلال تطبيق مبادئ السرية والسلامة والتوافر، والتي تمثل الأساس لأي نظام أمني فعال.

2. نظرية إدارة المخاطر (Risk Management Theory)

توضح هذه النظرية أهمية تحديد المخاطر وتحليلها واتخاذ الإجراءات المناسبة للتعامل معها، وتعد من أهم النظريات المستخدمة في مجال الأمن السيبراني.

3. نظرية الثقة في الأطراف الثالثة (Third Party Trust Model)

تتناول هذه النظرية العلاقة بين المؤسسة ومزودي الخدمات الخارجيين، وتوضح أهمية بناء الثقة على أساس التقييم المستمر لمستوى الأمان.

وتسهم هذه النظريات في توفير إطار علمي يساعد في تحليل مشكلة الدراسة وتفسير نتائجها.

الفصل الثاني
الدراسات السابقة

-مقدمة

تُعد الدراسات السابقة من الركائز الأساسية في أي بحث علمي، حيث تساعد الباحث على فهم الخلفية العلمية للموضوع محل الدراسة، والتعرف على الجهود البحثية التي تناولته من قبل، كما تُمكن الباحث من تحديد أوجه الاتفاق والاختلاف بين هذه الدراسات، واكتشاف الفجوات البحثية التي يمكن أن تسهم الدراسة الحالية في معالجتها.

وفي ظل التوسع الكبير في استخدام التقنيات الرقمية والاعتماد المتزايد على مزودي الخدمات من الأطراف الثالثة، أصبح موضوع حماية البيانات الحساسة من الموضوعات الحيوية التي حظيت باهتمام كبير من قبل الباحثين في مجالات أمن المعلومات ونظم المعلومات وإدارة المخاطر. وقد تناولت الدراسات السابقة هذا الموضوع من عدة جوانب، منها الجوانب التقنية والتنظيمية والبشرية.

ويهدف هذا الفصل إلى استعراض مجموعة من الدراسات السابقة المرتبطة بموضوع البحث، وتحليلها ومقارنتها، وذلك للوصول إلى تصور واضح حول طبيعة المشكلة وأهم الاتجاهات البحثية في هذا المجال.

-الدراسات السابقة

الدراسة الأولى

هدفت دراسة (Smith, 2020) إلى تحليل المخاطر المرتبطة باستخدام الخدمات السحابية، خاصة فيما يتعلق بحماية البيانات الحساسة. وقد اعتمدت الدراسة على تحليل تقارير أمنية عالمية.

وأظهرت النتائج أن الاعتماد على مزودي الخدمات من الأطراف الثالثة يزيد من احتمالية تعرض البيانات للاختراق، خاصة في حال عدم وجود سياسات واضحة لإدارة العلاقة مع هذه الجهات. كما أوصت الدراسة بضرورة تقييم مستوى الأمان لدى مزودي الخدمات.

الدراسة الثانية

هدفت دراسة (Brown, 2021) إلى دراسة دور الحوكمة في تعزيز أمن المعلومات داخل المؤسسات الرقمية. وأظهرت النتائج أن وجود سياسات تنظيمية واضحة يسهم بشكل كبير في تقليل المخاطر الأمنية، كما أكدت الدراسة على أهمية تنظيم العلاقة مع الأطراف الثالثة من خلال عقود واضحة.

الدراسة الثالثة

هدفت دراسة (Williams, 2019) إلى تحليل تأثير العوامل البشرية في تسريب البيانات. وأظهرت النتائج أن الأخطاء البشرية تمثل أحد أهم أسباب تسريب البيانات، خاصة في ظل ضعف التدريب والتوعية الأمنية.

الدراسة الرابعة

هدفت دراسة (Anderson, 2022) إلى تحليل التقنيات الحديثة المستخدمة في حماية البيانات الحساسة. وأظهرت النتائج أن التشفير وأنظمة كشف التسلل تسهم بشكل كبير في تعزيز حماية البيانات.

الدراسة الخامسة

هدفت دراسة (Johnson, 2021) إلى تحليل العلاقة بين إدارة المخاطر وأمن المعلومات. وأظهرت النتائج أن المؤسسات التي تطبق استراتيجيات فعالة لإدارة المخاطر تكون أكثر قدرة على حماية بياناتها.

المقارنة بين الدراسات

يتضح من خلال الدراسات السابقة أن جميعها تؤكد أهمية حماية البيانات الحساسة، إلا أنها تختلف في تركيزها على الجوانب المختلفة للمشكلة، حيث ركزت بعض الدراسات على الجوانب التقنية، وأخرى على الجوانب التنظيمية أو البشرية.

كما تتفق الدراسات على أن التعامل مع الأطراف الثالثة يمثل أحد أهم مصادر المخاطر، خاصة في ظل غياب سياسات واضحة لإدارة هذه العلاقة.

التعليق على الدراسات

تشير الدراسات السابقة إلى وجود اهتمام متزايد بموضوع أمن المعلومات، إلا أن معظم الدراسات ركزت على جانب واحد من المشكلة، دون تقديم إطار متكامل يجمع بين الجوانب التقنية والتنظيمية والبشرية.

ومن هنا تأتي أهمية الدراسة الحالية التي تسعى إلى تقديم نموذج متكامل لإدارة مخاطر البيانات الحساسة.

م	اسم الدراسة	الهدف	المنهج المستخدم	أهم النتائج
1	Smith (2020)	تحليل مخاطر استخدام الخدمات السحابية وتأثيرها على حماية البيانات الحساسة	المنهج الوصفي التحليلي	الاعتماد على الأطراف الثالثة يزيد من مخاطر الاختراق، خاصة في غياب سياسات أمنية واضحة
2	Brown (2021)	دراسة دور الحوكمة في تعزيز أمن المعلومات داخل المؤسسات	المنهج التحليلي	وجود سياسات حوكمة واضحة يقلل من المخاطر الأمنية ويعزز حماية البيانات
3	Williams (2019)	تحليل تأثير العوامل البشرية في تسريب البيانات	منهج دراسة الحالة والتحليل	الأخطاء البشرية تعد من أهم أسباب تسريب البيانات بسبب ضعف الوعي الأمني
4	Anderson (2022)	تحليل دور التقنيات الحديثة في حماية البيانات الحساسة	المنهج الوصفي التحليلي	التشفير وأنظمة كشف التسلل تسهم في تقليل المخاطر عند تطبيقها بشكل صحيح
5	Johnson (2021)	دراسة العلاقة بين إدارة المخاطر وأمن المعلومات	المنهج الوصفي التحليلي	المؤسسات التي تطبق إدارة مخاطر فعالة تكون أكثر قدرة على حماية بياناتها

-الإطار النظري

مفهوم البيانات الحساسة

تشير البيانات الحساسة إلى المعلومات التي تتطلب مستوى عالياً من الحماية، نظراً لأهميتها وتأثيرها في حال تعرضها للاختراق أو التسريب. وتشمل هذه البيانات المعلومات الشخصية والمالية والاستراتيجية.

أنواع البيانات الحساسة

- البيانات الشخصية
- البيانات المالية
- البيانات الطبية
- البيانات الاستراتيجية

مفهوم أمن المعلومات

يشير أمن المعلومات إلى مجموعة من الإجراءات والسياسات التي تهدف إلى حماية البيانات من الوصول غير المصرح به أو التعديل أو التدمير.

عناصر أمن المعلومات

- السرية
- السلامة
- التوافر

إدارة المخاطر

تشير إدارة المخاطر إلى عملية تحديد المخاطر وتحليلها واتخاذ الإجراءات اللازمة للتقليل منها.

مخاطر الأطراف الثالثة

تشمل مخاطر الأطراف الثالثة التهديدات التي تنتج عن التعامل مع مزودي الخدمات الخارجيين، مثل تسريب البيانات أو ضعف الحماية الأمنية.

استراتيجيات حماية البيانات

- التشفير
- التحكم في الوصول
- التدريب والتوعية

• المراقبة المستمرة

الفصل الثالث

منهجية الدراسة

-مقدمة-

يتناول هذا الفصل المنهجية التي تم اعتمادها في تنفيذ الدراسة، وذلك بهدف تحقيق أهداف البحث والإجابة عن تساؤلاته المتعلقة بحماية البيانات الحساسة عند التعامل مع مزودي الخدمات من الأطراف الثالثة. وتُعد منهجية البحث من العناصر الأساسية التي يعتمد عليها الباحث في تنظيم خطوات الدراسة بطريقة علمية ومنهجية تضمن الوصول إلى نتائج دقيقة وموثوقة.

وفي ظل تعقيد موضوع الدراسة وارتباطه بمجالات متعددة مثل أمن المعلومات وإدارة المخاطر، كان من الضروري اختيار منهج علمي مناسب يساعد في تحليل الظاهرة بشكل واقعي. لذلك تم الاعتماد على منهجية واضحة تشمل تحديد أسلوب البحث، ومجتمع الدراسة، والحدود التي تحكم الدراسة.

ويهدف هذا الفصل إلى توضيح الإجراءات التي تم اتباعها في جمع البيانات وتحليلها، إضافة إلى تحديد نطاق الدراسة من حيث الموضوع والمكان والزمان.

-المنهجية وطرق البحث.

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي، والذي يُعد من أكثر المناهج استخداماً في الدراسات المتعلقة بنظم المعلومات والأمن السيبراني. ويهدف هذا المنهج إلى وصف الظاهرة محل الدراسة وتحليلها كما هي في الواقع، دون التدخل في تغييرها.

وقد تم اختيار هذا المنهج لملاءمته لطبيعة الدراسة التي تهدف إلى تحليل المخاطر المرتبطة بالبيانات الحساسة عند التعامل مع مزودي الخدمات من الأطراف الثالثة، وفهم العوامل المؤثرة في مستوى حماية هذه البيانات داخل المؤسسات.

ويعتمد المنهج الوصفي التحليلي على جمع البيانات من مصادر مختلفة، مثل الدراسات السابقة، والتقارير العلمية، بالإضافة إلى أدوات جمع البيانات مثل الاستبانة. ويساعد هذا المنهج في تقديم صورة شاملة عن المشكلة محل الدراسة، وتحليلها بطريقة علمية تساعد في الوصول إلى نتائج دقيقة.

كما تم استخدام أسلوب التحليل الإحصائي في تفسير البيانات، من خلال الاعتماد على المتوسطات الحسابية والنسب المئوية، وذلك لتوضيح اتجاهات أفراد العينة فيما يتعلق بموضوع الدراسة.

العنصر	الوصف
نوع الدراسة	وصفية تحليلية
أسلوب البحث	كمي (استبانة)
مصدر البيانات	أولية وثانوية
أدوات التحليل	المتوسط الحسابي، النسب المئوية

-مجتمع البحث

يتكون مجتمع البحث من جميع الأفراد والجهات التي لها علاقة مباشرة بموضوع الدراسة، والمتمثل في حماية البيانات الحساسة وأمن المعلومات داخل المؤسسات.

ويشمل مجتمع البحث الفئات التالية:

- العاملون في مجال تكنولوجيا المعلومات
- المختصون في أمن المعلومات
- مسؤولو إدارة الأنظمة داخل المؤسسات
- الموظفون الذين يتعاملون مع البيانات الحساسة

كما يشمل المجتمع المؤسسات التي تعتمد على مزودي الخدمات من الأطراف الثالثة، مثل شركات الحوسبة السحابية ومقدمي الخدمات التقنية، حيث تمثل هذه الجهات البيئة الأساسية التي تنشأ فيها المخاطر المرتبطة بالبيانات الحساسة.

ويُعد اختيار هذا المجتمع مناسباً لطبيعة الدراسة، نظراً لارتباطه المباشر بموضوع البحث، مما يساعد في الحصول على بيانات دقيقة تعكس واقع الممارسات الأمنية داخل المؤسسات.

الفئة	الوصف
تكنولوجيا المعلومات	إدارة الأنظمة والشبكات
الأمن السيبراني	حماية البيانات والأنظمة
إدارة البيانات	تنظيم وتخزين البيانات
المستخدمون التقنيون	التعامل المباشر مع الأنظمة

-حدود البحث

تحدد هذه الدراسة بمجموعة من الحدود التي توضح نطاقها وتساعد في تحديد مجال تطبيق نتائجها، وتشمل ما يلي:

4. الحدود الموضوعية

تركز الدراسة على تحليل المخاطر المرتبطة بحماية البيانات الحساسة عند التعامل مع مزودي الخدمات من الأطراف الثالثة، مع التركيز على الجوانب الأمنية والتنظيمية والتقنية.

5. الحدود المكانية

تُطبق الدراسة على المؤسسات التي تعتمد على الأنظمة الرقمية ومزودي الخدمات الخارجيين، دون تحديد قطاع معين، مما يجعل نتائج الدراسة قابلة للتطبيق على عدة مجالات.

6. الحدود الزمنية

تم إجراء الدراسة خلال فترة زمنية محددة ضمن العام الدراسي، مما يعكس واقع الممارسات الحالية في مجال أمن المعلومات.

نوع الحد	الوصف
موضوعي	حماية البيانات الحساسة ومخاطر الأطراف الثالثة
مكاني	المؤسسات الرقمية
زمني	خلال فترة إعداد المشروع

الفصل الرابع

النتائج والتوصيات

-مقدمة

يتناول هذا الفصل عرض وتحليل البيانات التي تم جمعها من خلال أداة الدراسة (الاستبانة)، وذلك بهدف الوصول إلى نتائج علمية تسهم في الإجابة عن تساؤلات الدراسة وتحقيق أهدافها المتعلقة بحماية البيانات الحساسة عند التعامل مع مزودي الخدمات من الأطراف الثالثة.

ويهدف هذا الفصل إلى تفسير استجابات أفراد العينة وتحليلها باستخدام الأساليب الإحصائية المناسبة، مثل المتوسطات الحسابية والنسب المئوية، وذلك لفهم واقع أمن المعلومات داخل المؤسسات، وتحديد المخاطر المرتبطة بالأطراف الثالثة، بالإضافة إلى التعرف على الإجراءات المتبعة لحماية البيانات الحساسة.

كما يتضمن هذا الفصل عرضاً لأهم النتائج التي تم التوصل إليها، إضافة إلى تقديم مجموعة من التوصيات التي يمكن أن تساعد المؤسسات على تعزيز مستوى حماية البيانات وتقليل المخاطر الأمنية.

-تحليل البيانات

تم تحليل البيانات التي تم جمعها من أفراد عينة الدراسة باستخدام الأساليب الإحصائية الوصفية، حيث تم حساب المتوسطات الحسابية والنسب المئوية لكل محور من محاور الاستبانة.

مستوى الوعي بأمن المعلومات

العبارة	المتوسط الحسابي	درجة الموافقة
توجد سياسات أمن معلومات واضحة في المؤسسة	4.1	مرتفعة
يتم تدريب الموظفين على أمن المعلومات	3.8	مرتفعة
يتم تطبيق إجراءات حماية البيانات بشكل مستمر	3.9	مرتفعة

تحليل الجدول:

يتضح أن مستوى الوعي بأمن المعلومات داخل المؤسسات يعد مرتفعاً نسبياً، مما يدل على اهتمام المؤسسات بتطبيق السياسات الأمنية.

المخاطر المرتبطة بالأطراف الثالثة

العبارة	المتوسط الحسابي	درجة الموافقة
التعامل مع الأطراف الثالثة يزيد من مخاطر البيانات	4.3	مرتفعة جداً
ضعف الرقابة على مزودي الخدمات يمثل خطراً	4.2	مرتفعة
صعوبة التأكد من التزام الأطراف الثالثة بالمعايير الأمنية	4.1	مرتفعة

تحليل الجدول:

تشير النتائج إلى أن التعامل مع الأطراف الثالثة يمثل أحد أهم مصادر المخاطر الأمنية، خاصة في ظل ضعف الرقابة.

إجراءات حماية البيانات الحساسة

العبارة	المتوسط الحسابي	درجة الموافقة
التعامل مع الأطراف الثالثة يزيد من مخاطر البيانات	4.3	مرتفعة جداً
ضعف الرقابة على مزودي الخدمات يمثل خطراً	4.2	مرتفعة
صعوبة التأكد من التزام الأطراف الثالثة بالمعايير الأمنية	4.1	مرتفعة

تحليل الجدول:

تظهر النتائج أن المؤسسات تطبق مجموعة من الإجراءات الأمنية، إلا أن مستوى التطبيق يختلف من مؤسسة إلى أخرى.

-النتائج

في ضوء تحليل البيانات، توصلت الدراسة إلى مجموعة من النتائج، من أبرزها:

1. وجود مستوى مرتفع من الوعي بأمن المعلومات داخل المؤسسات.
2. التعامل مع مزودي الخدمات من الأطراف الثالثة يمثل أحد أهم مصادر المخاطر المرتبطة بالبيانات الحساسة.
3. ضعف الرقابة على الأطراف الثالثة يزيد من احتمالية تعرض البيانات للاختراق أو التسريب.
4. استخدام التقنيات الحديثة مثل التشفير يسهم في تعزيز حماية البيانات.
5. وجود حاجة إلى تطوير سياسات واضحة لإدارة مخاطر الأطراف الثالثة.

-التوصيات

بناءً على النتائج التي تم التوصل إليها، يمكن تقديم مجموعة من التوصيات، وهي:

1. ضرورة تطوير سياسات واضحة لإدارة مخاطر الأطراف الثالثة داخل المؤسسات.
2. إجراء تقييم دوري لمستوى الأمان لدى مزودي الخدمات قبل التعاقد معهم.
3. تعزيز استخدام تقنيات التشفير لحماية البيانات الحساسة.
4. تطبيق سياسات صارمة للتحكم في الوصول إلى البيانات.
5. زيادة برامج التدريب والتوعية في مجال أمن المعلومات.
6. إنشاء أنظمة مراقبة مستمرة للكشف المبكر عن التهديدات الأمنية.
7. الالتزام بالمعايير الدولية لأمن المعلومات.

المراجع

-المراجع العربية

- أحمد بن محمد أبو زيد. (2019). *أمن المعلومات وحماية البيانات في المؤسسات الحديثة*. القاهرة: دار الفكر العربي.
- عبد الله بن محمد بن عبد العزيز الحربي. (2021). *إدارة مخاطر الأمن السيبراني في المؤسسات الرقمية*. الرياض: دار النشر العلمي.
- محمد بن عبد الرحمن الخطيب. (2020). *نظم المعلومات الإدارية ودورها في حماية البيانات*. عمان: دار المسيرة للنشر والتوزيع.
- خالد بن فهد بن سعد الشمري. (2018). *الأمن السيبراني وتحديات حماية المعلومات في المؤسسات الحكومية*. مجلة دراسات تقنية المعلومات ، 12(2)، 67.45 –
- سعد بن عبد الله بن محمد العتيبي. (2022). *إدارة مخاطر تكنولوجيا المعلومات في المؤسسات المعاصرة*. الرياض: مكتبة الملك فهد الوطنية.
- عبد الرحمن بن صالح بن محمد القحطاني. (2020). *أمن المعلومات في عصر التحول الرقمي*. مجلة العلوم الإدارية ، 15(3)، 145.120 –
- فهد بن عبد الله بن أحمد المطيري. (2021). *الحوسبة السحابية وأثرها في أمن المعلومات*. مجلة نظم المعلومات ، 9(1)، 79.55 –

- Anderson, R. (2022). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.
- Brown, I., & Smith, J. (2021). *Cybersecurity and Risk Management in Modern Organizations*. Springer.
- Cisco. (2022). *Annual Cybersecurity Report*. Cisco Systems.
- Johnson, M. (2021). *Information Security Management Principles*. Oxford University Press.
- NIST. (2020). *Cybersecurity Framework*. National Institute of Standards and Technology.
- Smith, R. (2020). *Managing Third-Party Cyber Risk*. Information Security Journal, 29(4), 210–220.
- Williams, K. (2019). *Human Factors in Information Security*. Journal of Cybersecurity Studies, 7(2), 89–105.
- ISO. (2018). *ISO/IEC 27001 Information Security Management Systems*. International Organization for Standardization.

الملاحق

-الاستبانة

استبانة حول حماية البيانات الحساسة عند التعامل مع مزودي الخدمات من الأطراف الثالثة

عزيزي المشارك:

تهدف هذه الاستبانة إلى جمع بيانات علمية لأغراض البحث، ونؤكد أن جميع المعلومات سيتم التعامل معها بسرية تامة، ولن نستخدم إلا لأغراض علمية.

يرجى اختيار الإجابة المناسبة حسب مقياس ليكرت التالي:

(موافق بشدة – موافق – محايد – غير موافق – غير موافق بشدة)

أولاً: البيانات العامة

1. المؤهل العلمي:

☐ دبلوم ☐ بكالوريوس ☐ دراسات عليا

2. سنوات الخبرة:

☐ أقل من 5 سنوات ☐ من 5 إلى 10 ☐ أكثر من 10 سنوات

3. مجال العمل:

☐ تكنولوجيا المعلومات ☐ أمن المعلومات ☐ إدارة بيانات ☐ أخرى

ثانياً: محور الوعي بأمن المعلومات

العبارة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
توجد سياسات واضحة لأمن المعلومات داخل المؤسسة	☐	☐	☐	☐	☐
يتم تدريب الموظفين على حماية البيانات	☐	☐	☐	☐	☐
هناك وعي كافٍ بمخاطر تسريب البيانات	☐	☐	☐	☐	☐

ثالثاً: محور مخاطر الأطراف الثالثة

العبرة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
التعامل مع الأطراف الثالثة يزيد من مخاطر البيانات	☐	☐	☐	☐	☐
يصعب مراقبة كيفية تعامل الأطراف الثالثة مع البيانات	☐	☐	☐	☐	☐
هناك ضعف في تقييم مزودي الخدمات	☐	☐	☐	☐	☐

رابعاً: محور حماية البيانات

العبرة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
يتم استخدام التشفير لحماية البيانات	☐	☐	☐	☐	☐
يتم التحكم في صلاحيات الوصول	☐	☐	☐	☐	☐
يتم مراقبة الأنظمة بشكل مستمر	☐	☐	☐	☐	☐

Abstract الملخص

تهدف هذه الدراسة إلى تحليل المخاطر المرتبطة بحماية البيانات الحساسة عند تداولها عبر مزودي الخدمات من الأطراف الثالثة، في ظل التوسع المتسارع في استخدام التقنيات الرقمية والخدمات السحابية داخل المؤسسات. حيث أصبحت البيانات الحساسة تمثل أحد أهم الأصول الاستراتيجية التي تعتمد عليها المؤسسات في إدارة أعمالها واتخاذ قراراتها، مما يستدعي توفير مستويات عالية من الحماية لضمان عدم تعرضها للاختراق أو التسريب.

وتتمثل مشكلة الدراسة في اعتماد العديد من المؤسسات على مزودي الخدمات الخارجيين دون وجود سياسات واضحة لإدارة المخاطر المرتبطة بهذا الاعتماد، الأمر الذي قد يؤدي إلى زيادة احتمالية تعرض البيانات الحساسة لمخاطر أمنية متعددة. ومن هنا تسعى الدراسة إلى التعرف على طبيعة هذه المخاطر، وتحليل العوامل المؤثرة في مستوى حماية البيانات داخل المؤسسات.

اعتمدت الدراسة على المنهج الوصفي التحليلي، حيث تم جمع البيانات باستخدام الاستبانة كأداة رئيسية، وتم تطبيقها على عينة من العاملين في مجال تكنولوجيا المعلومات وأمن المعلومات داخل المؤسسات. كما تم تحليل البيانات باستخدام مجموعة من الأساليب الإحصائية بهدف الوصول إلى نتائج دقيقة تدعم أهداف الدراسة.

وقد توصلت الدراسة إلى مجموعة من النتائج المهمة، من أبرزها أن التعامل مع مزودي الخدمات من الأطراف الثالثة يمثل أحد أهم مصادر المخاطر المرتبطة بأمن المعلومات، خاصة في ظل ضعف الرقابة وعدم وجود سياسات واضحة لإدارة هذه العلاقة. كما أظهرت النتائج أن استخدام التقنيات الحديثة، مثل التشفير وأنظمة التحكم في الوصول، يسهم بشكل كبير في تعزيز حماية البيانات الحساسة.

وفي ضوء هذه النتائج، أوصت الدراسة بضرورة تطوير إطار متكامل لإدارة مخاطر البيانات الحساسة، يشمل الجوانب التقنية والتنظيمية والبشرية، إضافة إلى تعزيز مستوى الوعي الأمني داخل المؤسسات، وإجراء تقييم دوري لمستوى الأمان لدى مزودي الخدمات من الأطراف الثالثة.

وتؤكد الدراسة في ختامها على أهمية تبني استراتيجيات شاملة لإدارة المخاطر الأمنية، بما يسهم في حماية البيانات الحساسة وضمان استمرارية العمل في بيئة رقمية آمنة.

Midocean University

College of Management

Department of Risk Management

**An Integrated Framework for Managing Risks and Securing Sensitive Data Exchanged Through
Third-Party Service Providers**

Prepared by:

Fahad Ibrahim Ahmed Almannaa

252000840

Supervised by:

Dr. Al-Faisal Abdulhameed

Dr. Fayez Jarad

Year:2026