

دور التكنولوجيا الحديثة في تحسين عمليات إدارة المخاطر والتهديدات الإلكترونية وأساليب الحماية

إعداد الطالبة /
سارة أحمد القحطاني

(243001145)

إشراف /
د. الفيصل عبد الحميد محمد حسن
د. فايز جراد

العام الدراسي:
2025-2024

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

إهداء

أهدي هذا العمل إلى والدي الكريمين اللذين كان لي النبراس والداعم الأكبر في حياتي إلى والدتي الكنونة: التي غرست في حب العلم والمعرفة، وإلى والدي العزيز، الذي علّمني قوة الإرادة والمثابرة.

إلى أساتذتي الأفاضل، الذين لم ييخلوا عليّ بعلمهم وتوجيهاتهم. فقد كان نخبرتهم وإرشاداتهم الأثر الكبير في إنجاز هذا العمل.

إلى زملائي وأصدقائي الأعزاء الذين شاركوني التحديات والنجاحات، أهدي هذا العمل تعبيراً عن شكري وامتناني لكل دعمهم وتشجيعهم.

وأخيراً، أهدي هذا العمل إلى كل من ساهم في دعمي وتشجيعي، سائلاً الله أن يجعل هذا الإنجاز بداية لمزيد من النجاحات والتقدم.

شُكْرٌ وَتَقْدِيرٌ

الحمد لله الذي بنعمته تتم الصالحات، والصلاة والسلام على سيد الخلق محمد وعلى آله وصحبه أجمعين.

أقدم بخالص الشكر والتقدير إلى والدي العزيزين، اللذين كانا لي الدعم الأكبر والأساس في كل

مراحل حياتي. إن إيمانهما بي ودعمهما المتواصل كانا الدافع وراء هذا الإنجاز.

أشكر أساتذتي الأفاضل، وبالأخص مشرفي الكريم، على توجيهاتهم السديدة وإرشاداتهم القيمة التي

ساعدتني على تطوير هذا البحث وإتمامه بنجاح.

د. الفیصل عبد الحکیم محمد حسن

د. فايز جراد

أود أيضاً أن أشكر زملائي وأصدقائي، الذين كانوا لي خير رفاق وداعمين، وشاركوا معي التحديات

والنجاحات. إن دعمهم وتشجيعهم كان له الأثر الإيجابي في تجاوز العقبات وتحقيق هذا النجاح

وفي الختام، أتوجه بالشكر لكل من ساهم بأي شكل في إنجاز هذا العمل، وكل من قدم لي الدعم أو

التشجيع. وأسأل الله أن يوفقنا جميعاً لما فيه الخير، وأن يجعل هذا العمل نافعاً ومثمراً.

المستخلص

تهدف هذه الدراسة إلى تحليل الدور الذي تؤديه التكنولوجيا الحديثة في تحسين إدارة المخاطر الإلكترونية داخل المؤسسات السعودية والعربية، من خلال التعرف على مستوى تبني هذه المؤسسات للتقنيات المتقدمة مثل الذكاء الاصطناعي وتحليلات البيانات الضخمة، وقدرتها على كشف التهديدات الإلكترونية والاستجابة لها بشكل فعال. جاءت أهمية هذه الدراسة من الحاجة الماسة إلى تعزيز الأمان السيبراني في المؤسسات لمواجهة تصاعد التهديدات الإلكترونية المعقدة التي قد تؤثر سلبًا على استمرارية الأعمال وسمعة المؤسسات.

اعتمدت الدراسة المنهج الوصفي التحليلي، وتم تصميم أداة لجمع البيانات تمثلت في استبانة إلكترونية شاملة وزعت على عينة مكونة من 250 موظفًا من العاملين في أقسام تقنية المعلومات والأمن السيبراني في مؤسسات حكومية وخاصة بمختلف الأحجام. تم تحليل البيانات باستخدام الإحصاءات الوصفية والاستدلالية بما في ذلك اختبار T وتحليل التباين ANOVA وتحليل الارتباط، كما تم التحقق من صلاحية البيانات من خلال اختبارات التوزيع الطبيعي وتجارب الثبات.

أظهرت نتائج الدراسة وجود علاقة ارتباط موجبة قوية ودالة إحصائيًا بين مستوى توظيف التكنولوجيا الحديثة وفعالية إدارة المخاطر الإلكترونية، كما أوضحت وجود فروق ذات دلالة إحصائية تعزى لمتغير حجم المؤسسة، حيث أظهرت المؤسسات الكبيرة مستويات أعلى من الكفاءة في إدارة المخاطر الإلكترونية مقارنة بالمؤسسات الصغيرة والمتوسطة. وبينت النتائج كذلك أن من أبرز التحديات التي تعيق توظيف التكنولوجيا بشكل فعال هي التحديات البشرية والتنظيمية مثل نقص الكفاءات المتخصصة وصعوبة دمج الحلول التقنية مع الأنظمة القائمة.

أوصت الدراسة بتطوير خطط تدريبية دورية للكوادر المتخصصة، وتخصيص ميزانيات مستقلة للأمن السيبراني، وتحديث السياسات الأمنية بانتظام، إضافة إلى العمل على تعزيز التكامل بين الأنظمة التقنية المختلفة والتعاون مع الجهات الوطنية المختصة بالأمن السيبراني لضمان تحقيق حماية شاملة وفعالة للأصول الرقمية للمؤسسات وضمان استمرارية أعمالها في ظل التهديدات الإلكترونية المتزايدة.

الكلمات المفتاحية:

الأمن السيبراني، إدارة المخاطر الإلكترونية، التكنولوجيا الحديثة، الذكاء الاصطناعي، المؤسسات السعودية، الحلول التقنية.

قائمة المحتويات

ب.....	بسم الله الرحمن الرحيم
ت.....	إهداء
ث.....	شكر وتقدير
ج.....	المستخلص
ح.....	قائمة المحتويات
ذ.....	قائمة الجداول
ر.....	قائمة الأشكال
1.....	الفصل الأول الإطار العام للدراسة
1.....	1.1 المقدمة
2.....	2.1 مشكلة الدراسة
3.....	3.1 أهمية الدراسة
4.....	4.1 أهمية الدراسة
4.....	جدول 3: أبعاد أهمية الدراسة
5.....	5.1 فروض الدراسة
5.....	جدول 4: فروض الدراسة
6.....	6.1 نموذج الدراسة
6.....	• وصف مكونات نموذج الدراسة
7.....	7.1 الدراسات السابقة
9.....	8.1 المنطلقات النظرية للدراسة
9.....	9.1 المنهجية وطرق البحث
11.....	11.1 مصادر البيانات
12.....	12.1 أدوات الدراسة
13.....	13.1 حدود الدراسة
15.....	الفصل الثاني: الإطار النظري
15.....	تمهيد
15.....	1.2 المبحث الأول: مفاهيم إدارة المخاطر الإلكترونية
15.....	1.1.2 مقدمة
16.....	2.1.2 التطور التاريخي لإدارة المخاطر الإلكترونية
16.....	3.1.2 تعريف المخاطر الإلكترونية
17.....	4.1.2 تعريف إدارة المخاطر الإلكترونية
17.....	5.1.2 أهمية إدارة المخاطر الإلكترونية في المؤسسات الحديثة
18.....	6.1.2 أهداف إدارة المخاطر الإلكترونية
19.....	7.1.2 أسباب تزايد الحاجة لإدارة المخاطر الإلكترونية في العصر الرقمي
20.....	8.1.2 أبعاد إدارة المخاطر الإلكترونية

21	2.2 المبحث الثاني: التكنولوجيا الحديثة ودورها في إدارة المخاطر الإلكترونية
21	1.2.2 مقدمة
21	2.2.2 تعريف التكنولوجيا الحديثة في مجال الأمن السيبراني
22	3.2.2 أهمية التكنولوجيا الحديثة في تحسين إدارة المخاطر الإلكترونية
23	4.2.2 أهداف توظيف التكنولوجيا الحديثة لحماية الأصول الرقمية
24	5.2.2 مراحل تطبيق التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية
25	6.2.2 العقبات التي تواجه المؤسسات في تطبيق التكنولوجيا الحديثة للأمن السيبراني
26	7.2.2 خصائص الحلول التقنية الفعالة في إدارة المخاطر الإلكترونية
28	7.2.2 التطور التاريخي للتكنولوجيا الحديثة في المجال السيبراني
29	8.2.2 أبعاد توظيف التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية
31	الفصل الثالث: المنهجية والإجراءات
31	تمهيد
31	3.1 منهج الدراسة
31	3.2 مجتمع وعينة الدراسة
31	3.3 خصائص العينة الشخصية والوظيفية
33	□ خصائص العينة حسب المؤهل العلمي
34	□ خصائص العينة حسب سنوات الخبرة
35	3.4 أداة الدراسة
35	3.5 الأساليب الإحصائية المستخدمة
37	الفصل الرابع: تحليل البيانات واختبار الفرضيات
37	4.1 المقدمة
37	نتائج اختبار التوزيع الطبيعي:
38	4.3 التحليل الوصفي لبيانات الدراسة
39	جدول 4.2 التحليل الوصفي لمحاو الاستبانة
39	4.4 الاختبارات القبلية للأداة
39	أولاً: صدق الأداة (Validity)
39	ثانياً: ثبات الأداة (Reliability)
40	4.4.5 اختبار فرضيات الدراسة
41	اختبار الفرضيات المتعلقة بالفروق حسب المتغيرات التصنيفية
41	جدول 4.5 نتائج اختبار الفروق حسب الخصائص الشخصية والوظيفية
42	الفصل الخامس: مناقشة النتائج والتوصيات
42	5.1 المقدمة
42	5.2 النتائج المتعلقة بمتغيرات الدراسة الوصفية
43	5.3 النتائج المتعلقة باختبار فرضيات الدراسة
43	مقارنة نتائج الدراسة الحالية بالدراسات السابقة
44	5.4 التوصيات
I	Abstract
II	المراجع

II	قائمة المراجع العربية.....
II	قائمة المراجع الإنجليزية.....
IV	أولاً: البيانات الشخصية والوظيفية
IV	ثانيًا: محاور الاستبانة (مقياس ليكرت الخماسي).....

قائمة الجداول

رقم الصفحة	اسم الجدول
2	1: جدول أوجه القصور في إدارة المخاطر الإلكترونية بالمؤسسات
3	جدول 2: أبعاد أهمية الدراسة
4	جدول 3: أبعاد أهمية الدراسة
5	جدول 4: فروض الدراسة
7	جدول 5: وصف عناصر نموذج الدراسة
8	جدول 6: مقارنة بين الدراسات السابقة
9	جدول 7: المنطلقات النظرية ودورها في الدراسة
11	جدول 8: مراحل تنفيذ الدراسة
11	جدول 9: مصادر البيانات وأهمية كل منها
12	جدول 10: أدوات الدراسة واستخداماتها
13	جدول 11: الأساليب الإحصائية المستخدمة وأغراضها
14	جدول 12: حدود الدراسة وتأثيرها المحتمل
21	جدول 13: أبعاد إدارة المخاطر الإلكترونية
25	جدول 14: مراحل تطبيق التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية
26	جدول 15: العقبات التي تحد من تطبيق التكنولوجيا الحديثة
28	جدول 16: خصائص الحلول التقنية الفعالة
29	جدول 17: مراحل تطور التكنولوجيا الحديثة في المجال السيبراني
30	جدول 18: أبعاد توظيف التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية
32	جدول 3.1 توزيع العينة حسب النوع الاجتماعي
33	جدول 3.2 توزيع العينة حسب الفئة العمرية
34	جدول 3.3 توزيع العينة حسب المؤهل العلمي
34	جدول 3.4 توزيع العينة حسب سنوات الخبرة
38	جدول 4.1 اختبار التوزيع الطبيعي
39	جدول 4.2 التحليل الوصفي لمحاوَر الاستبانة
39	جدول 4.3 نتائج الثبات
41	جدول 4.5 نتائج اختبار الفروق حسب الخصائص الشخصية والوظيفية
44	جدول 5.1 مقارنة النتائج بالدراسات السابقة

قائمة الأشكال

رقم الصفحة	اسم الشكل
6	الشكل (1) توظيف التكنولوجيا الحديثة
32	شكل 3.1 توزيع حسب الجنس
33	شكل 3.2 توزيع حسب الفئة العمرية
34	شكل 3.3 توزيع حسب المؤهل العلمي
35	شكل 3.4 توزيع بحسب سنوات الخبرة

1.1 المقدمة

تشهد بيئة الأعمال والأنشطة الاقتصادية والاجتماعية تحولات متسارعة بفعل الثورة الرقمية وانتشار التكنولوجيا الحديثة، التي أصبحت حجر الزاوية في جميع جوانب الحياة اليومية. (Kshetri, 2019) ومع توسع الاعتماد على التقنيات الرقمية، ظهرت تحديات جديدة تتعلق بالمخاطر والتهديدات الإلكترونية التي باتت تشكل خطرًا حقيقيًا يهدد أمن المعلومات وسرية البيانات وسلامة الأنظمة الإلكترونية في المؤسسات بمختلف أنواعها، سواء كانت حكومية أو خاصة. (Von Solms & Van Niekerk, 2013)

لقد أسهم التطور الهائل في تكنولوجيا المعلومات والاتصالات في خلق بيئة إلكترونية ذات إمكانيات هائلة لتعزيز الكفاءة التشغيلية والابتكار في المؤسسات، غير أن هذا التطور رافقته مخاطر معقدة ومتعددة الأبعاد تتجاوز حدود الزمان والمكان، وتتمثل في الهجمات الإلكترونية، والبرمجيات الخبيثة، وعمليات الاختراق، والتصيد الإلكتروني، والابتزاز الرقمي، وغيرها من أشكال التهديدات السيبرانية التي تتطور بشكل مستمر. (Bada et al., 2019) وباتت هذه المخاطر تمثل تحديًا كبيرًا لإدارات المخاطر في المؤسسات، ما يفرض ضرورة تبني أساليب متطورة في الكشف المبكر، والوقاية، والاستجابة الفاعلة لهذه التهديدات. (ENISA, 2021)

وفي هذا السياق، أصبحت التكنولوجيا الحديثة ذات دور محوري في تحسين إدارة المخاطر الإلكترونية عبر أدوات وتقنيات متنوعة مثل الذكاء الاصطناعي، وتقنيات التعلم الآلي، وتحليلات البيانات الضخمة، وأنظمة إدارة أمن المعلومات، التي أسهمت في رفع مستوى الحماية الرقمية وكفاءة التصدي للهجمات الإلكترونية. (Sharma & Sahay, 2021) كما ساعدت هذه التقنيات في تقليل الآثار السلبية للمخاطر من خلال القدرة على التنبؤ بالتهديدات، واكتشاف الثغرات الأمنية، وتقديم حلول استباقية تقلل من احتمالية وقوع حوادث أمنية جسيمة. (Ammar et al., 2020)

ونظرًا لأهمية حماية الأصول الرقمية والبيانات الحساسة للمؤسسات، أصبحت الحاجة ملحة لإعداد دراسات متعمقة تبحث في كيفية توظيف التكنولوجيا الحديثة بأفضل صورة ممكنة في إدارة المخاطر الإلكترونية، وتطوير استراتيجيات وأساليب حماية فعالة وشاملة تتناسب مع طبيعة التهديدات المتجددة. (ISO/IEC, 2018) وتكتسب هذه الدراسة أهميتها من كونها تسعى إلى تسليط الضوء على التقنيات الحديثة المستخدمة في رصد وإدارة المخاطر الإلكترونية، وتقييم مدى فعاليتها في دعم المنظمات في مواجهة التهديدات الإلكترونية المتصاعدة. (ENISA, 2021)

وتتناول الدراسة بالدراسة والتحليل آليات توظيف التكنولوجيا الحديثة في تحسين قدرات الكشف المبكر عن المخاطر الإلكترونية، وطرق الاستجابة لها، كما تبحث في التحديات التي قد تواجه المؤسسات عند تطبيق هذه التقنيات، وأفضل الممارسات العالمية في مجال حماية المعلومات. (Sharma & Sahay, 2021) وتسعى هذه الدراسة لتقديم إطار علمي يساعد متخذي القرار في المؤسسات المختلفة على تطوير سياسات واستراتيجيات أكثر مرونة وفعالية لإدارة المخاطر الإلكترونية، بما يعزز استمرارية الأعمال ويحافظ على سمعة المؤسسة وثقة عملائها. (Bada et al., 2019)

2.1 مشكلة الدراسة

تشير الأدبيات الحديثة إلى أن اعتماد المؤسسات المتزايد على الأنظمة الرقمية ساهم بشكل كبير في تسريع الأداء وتحقيق الكفاءة التشغيلية، لكنه في المقابل كشف عن نقاط ضعف جديدة، حيث أصبحت الهجمات الإلكترونية أكثر تطوراً وخطورة، وتتنوع أساليبها بشكل يتجاوز القدرات التقليدية لأنظمة الحماية (Von Solms & Van Niekerk, 2013). وقد أدى ذلك إلى تزايد الخسائر الناجمة عن الحوادث السيبرانية، سواء على المستوى المالي أو

في سمعة المؤسسات وثقة العملاء فيها. (Bada et al., 2019)

إن المشكلة الجوهرية التي تعاني منها العديد من المؤسسات تكمن في عدم قدرتها على التنبؤ بالتهديدات الإلكترونية المتجددة أو الكشف المبكر عنها، نظراً لاعتمادها في معظم الأحيان على أساليب حماية تقليدية تركز على رد الفعل بعد وقوع الهجوم، بدلاً من تبني حلول استباقية متطورة. (ENISA, 2021) كما تفتقر الكثير من المؤسسات إلى السياسات الأمنية المرنة، والبرامج التدريبية الكافية لتطوير قدرات الكوادر البشرية على التعامل مع التهديدات المستجدة، ما يؤدي إلى توسيع الفجوة بين سرعة تطور الهجمات الإلكترونية ومستوى الحماية المطبق فعلياً في المؤسسة (Sharma & Sahay, 2021).

إضافة إلى ذلك، هناك تحديات متعلقة بارتفاع تكاليف الاستثمار في الحلول التقنية الحديثة وصعوبة دمجها مع الأنظمة القائمة، ما يزيد من احتمالية تعرض المؤسسات للاختراقات المتكررة. (Ammar et al., 2020) وتتفاقم المشكلة أكثر في المؤسسات الصغيرة والمتوسطة، التي غالباً ما تكون مواردها محدودة ولا تمتلك هيكلًا تنظيميًا متخصصاً في إدارة المخاطر الإلكترونية. (Kshetri, 2019)

وتتمثل مشكلة هذه الدراسة تحديداً في البحث عن إجابة للسؤال الرئيسي:

ما مدى قدرة المؤسسات السعودية والعربية على توظيف التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية بشكل فعال؟ وما العوامل التي تحد من قدرتها على تطبيق هذه الحلول التقنية بشكل كامل وفعال، بالرغم من توفرها في السوق؟

1: جدول أوجه القصور في إدارة المخاطر الإلكترونية بالمؤسسات

البند	الوصف
طبيعة أنظمة الحماية التقليدية	تعتمد على الكشف المتأخر، وتتطلب تدخلاً يدوياً
التدريب والكفاءات البشرية	نقص الخبرات المؤهلة للتعامل مع التهديدات الحديثة
تكامل الأنظمة	صعوبة ربط الحلول التقنية الحديثة بالأنظمة القائمة
الدعم الإداري	ضعف التوجه الاستراتيجي للأمن السيبراني في بعض المؤسسات
الميزانيات المخصصة	قلة الموارد المالية المرسودة للأمن السيبراني

يتضح مما سبق أن فجوة كبيرة لا تزال تفصل بين الإمكانيات الهائلة التي توفرها التكنولوجيا الحديثة وبين الواقع الفعلي لتطبيقها في مؤسساتنا، الأمر الذي يجعل الحاجة ماسة لإجراء دراسة علمية تسعى لتحليل أسباب هذه الفجوة واقتراح حلول عملية لسدها،

بما يعزز قدرات المؤسسات على حماية بياناتها وأصولها الرقمية بفعالية. (ISO/IEC, 2018)

3.1 أهمية الدراسة

في ظل تسارع وتيرة التحول الرقمي في المملكة العربية السعودية والمنطقة العربية، أرى أن أهمية هذه الدراسة تنبع من الحاجة الملحة لفهم كيفية توظيف التكنولوجيا الحديثة في تعزيز قدرة المؤسسات على حماية أصولها الرقمية وإدارة المخاطر الإلكترونية بكفاءة عالية. (ENISA, 2021) وقد لاحظت من خلال مراجعة الأدبيات والتقارير المتخصصة أن معظم المؤسسات في المنطقة ما تزال تعتمد على حلول تقليدية في أمن المعلومات، رغم توفر حلول تقنية متقدمة مثل الذكاء الاصطناعي وتقنيات التحليل السلوكي، والتي يمكن أن تحدث فرقاً جوهرياً في الكشف المبكر عن التهديدات وتقليل خسائرها. (Sharma & Sahay, 2021)

كما تكتسب دراستي أهميتها العلمية من كونها تسعى لسد فجوة بحثية واضحة في البيئة العربية؛ حيث إن أغلب الدراسات الحالية تركز على تجارب عالمية دون التطرق بعمق للخصوصية التشريعية والثقافية للمؤسسات المحلية (Kshetri, 2019) ومن خلال هذه الدراسة أسعى لتقديم نموذج تحليلي يوضح كيف يمكن دمج الحلول التقنية الحديثة ضمن بيئة العمل السعودية والعربية، وتحديد العوامل التي تدعم أو تحد من فاعليتها، بما يساعد صناع القرار في المؤسسات على تبني سياسات أمنية مرنة واستباقية.

كذلك أرى أن الدراسة تحمل أهمية عملية، حيث ستساهم نتائجها وتوصياتها في توجيه المؤسسات لتحديث استراتيجياتها الأمنية بما يتماشى مع متطلبات رؤية المملكة 2030، من خلال رفع الجاهزية السيبرانية وضمان استمرارية الأعمال والحفاظ على سمعة المؤسسات وثقة العملاء. (ISO/IEC, 2018) ومن منظور الباحث، فإن النتائج ستوفر بيانات ميدانية حديثة تساعد المهتمين والمختصين في تصميم برامج تدريبية وخطط تطويرية للكوادر الوطنية في مجال الأمن السيبراني.

البعد	التوضيح
الأهمية العلمية	إثراء الأدبيات العربية في مجال إدارة المخاطر الإلكترونية
الأهمية العملية	تقديم حلول واقعية قابلة للتطبيق في المؤسسات المحلية
الأهمية الاجتماعية	المساهمة في حماية بيانات الأفراد والمؤسسات وتعزيز الثقة الرقمية
الأهمية الاقتصادية	تقليل التكاليف الناتجة عن حوادث الاختراق والهجمات الإلكترونية
الأهمية الاستراتيجية	دعم توجهات الدولة في رفع الجاهزية السيبرانية ضمن رؤية 2030

جدول 2: أبعاد أهمية الدراسة

ومن خلال هذه الدراسة أسعى لتقديم مساهمة علمية وعملية في تحسين مستوى أمن المعلومات في بيئة الأعمال السعودية والعربية، بما يحقق توازنًا بين الاستفادة من مزايا التكنولوجيا الحديثة وتقليل المخاطر المصاحبة لها، عبر استراتيجيات مبنية على أسس علمية مدروسة. (Bada et al., 2019)

4.1 أهمية الدراسة

في ظل تسارع وتيرة التحول الرقمي في المملكة العربية السعودية والمنطقة العربية، أرى أن أهمية هذه الدراسة تنبع من الحاجة الملحة لفهم كيفية توظيف التكنولوجيا الحديثة في تعزيز قدرة المؤسسات على حماية أصولها الرقمية وإدارة المخاطر الإلكترونية بكفاءة عالية. (ENISA, 2021) وقد لاحظت من خلال مراجعة الأدبيات والتقارير المتخصصة أن معظم المؤسسات في المنطقة ما تزال تعتمد على حلول تقليدية في أمن المعلومات، رغم توفر حلول تقنية متقدمة مثل الذكاء الاصطناعي وتقنيات التحليل السلوكي، والتي يمكن أن تحدث فرقًا جوهريًا في الكشف المبكر عن التهديدات وتقليل خسائرها. (Sharma & Sahay, 2021)

كما تكتسب دراستي أهميتها العلمية من كونها تسعى لسد فجوة بحثية واضحة في البيئة العربية؛ حيث إن أغلب الدراسات الحالية تركز على تجارب عالمية دون التطرق بعمق للخصوصية التشريعية والثقافية للمؤسسات المحلية (Kshetri, 2019). ومن خلال هذه الدراسة أسعى لتقديم نموذج تحليلي يوضح كيف يمكن دمج الحلول التقنية الحديثة ضمن بيئة العمل السعودية والعربية، وتحديد العوامل التي تدعم أو تحد من فاعليتها، بما يساعد صناع القرار في المؤسسات على تبني سياسات أمنية مرنة واستباقية.

كذلك أرى أن الدراسة تحمل أهمية عملية، حيث ستساهم نتائجها وتوصياتها في توجيه المؤسسات لتحديث استراتيجياتها الأمنية بما يتماشى مع متطلبات رؤية المملكة 2030، من خلال رفع الجاهزية السيبرانية وضمان استمرارية الأعمال والحفاظ على سمعة المؤسسات وثقة العملاء. (ISO/IEC, 2018) ومن منظور الباحث، فإن النتائج ستوفر بيانات ميدانية حديثة تساعد المهتمين والمختصين في تصميم برامج تدريبية وخطط تطويرية للكوادر الوطنية في مجال الأمن السيبراني.

التوضيح	البعد
إثراء الأدبيات العربية في مجال إدارة المخاطر الإلكترونية	الأهمية العلمية
تقديم حلول واقعية قابلة للتطبيق في المؤسسات المحلية	الأهمية العملية
المساهمة في حماية بيانات الأفراد والمؤسسات وتعزيز الثقة الرقمية	الأهمية الاجتماعية
تقليل التكاليف الناتجة عن حوادث الاختراق والهجمات الإلكترونية	الأهمية الاقتصادية
دعم توجهات الدولة في رفع الجاهزية السيبرانية ضمن رؤية 2030	الأهمية الاستراتيجية

جدول 3: أبعاد أهمية الدراسة

ومن خلال هذه الدراسة أسعى لتقديم مساهمة علمية وعملية في تحسين مستوى أمن المعلومات في بيئة الأعمال السعودية والعربية، بما يحقق توازنًا بين الاستفادة من مزايا التكنولوجيا الحديثة وتقليل المخاطر المصاحبة لها، عبر استراتيجيات مبنية على أسس علمية مدروسة. (Bada et al., 2019)

5.1 فروض الدراسة

استنادًا إلى ما أسعى لتحقيقه في هذه الدراسة، أضع مجموعة من الفروض العلمية التي أرى أنها ضرورية لاختبار العلاقة بين توظيف التكنولوجيا الحديثة وفعالية إدارة المخاطر الإلكترونية في المؤسسات السعودية والعربية. وتتمثل هذه الفروض فيما يلي:

1. توجد فروق ذات دلالة إحصائية في فعالية إدارة المخاطر الإلكترونية بين المؤسسات التي تستخدم التكنولوجيا الحديثة وتلك التي تعتمد على الأساليب التقليدية.
2. يساهم توظيف تقنيات الذكاء الاصطناعي وتحليلات البيانات في تقليل زمن اكتشاف التهديدات الإلكترونية بشكل ملحوظ.
3. توجد علاقة موجبة ذات دلالة إحصائية بين مستوى جاهزية المؤسسة لتبني التكنولوجيا الحديثة وفعالية إدارتها للمخاطر الإلكترونية.
4. تشكل التحديات التنظيمية والبشرية والتقنية عائقًا أمام المؤسسات في توظيف الحلول التقنية الحديثة بكفاءة.
5. يساهم تصميم نموذج تطبيقي متكامل يجمع بين التكنولوجيا الحديثة والسياسات الأمنية المرنة في رفع جاهزية المؤسسات وتقليل الخسائر الناتجة عن الهجمات الإلكترونية.

رقم الفرض	نص الفرض
1	توجد فروق في الفعالية بين المؤسسات التي تستخدم التكنولوجيا الحديثة والأساليب التقليدية.
2	توظيف الذكاء الاصطناعي يساعد في تقليل زمن اكتشاف التهديدات.
3	هناك علاقة موجبة بين الجاهزية المؤسسية وفعالية إدارة المخاطر.
4	التحديات التنظيمية والبشرية والتقنية تحد من كفاءة التوظيف التقني.
5	النموذج المتكامل للتكنولوجيا والسياسات الأمنية يقلل الخسائر ويرفع الجاهزية.

جدول 4: فروض الدراسة

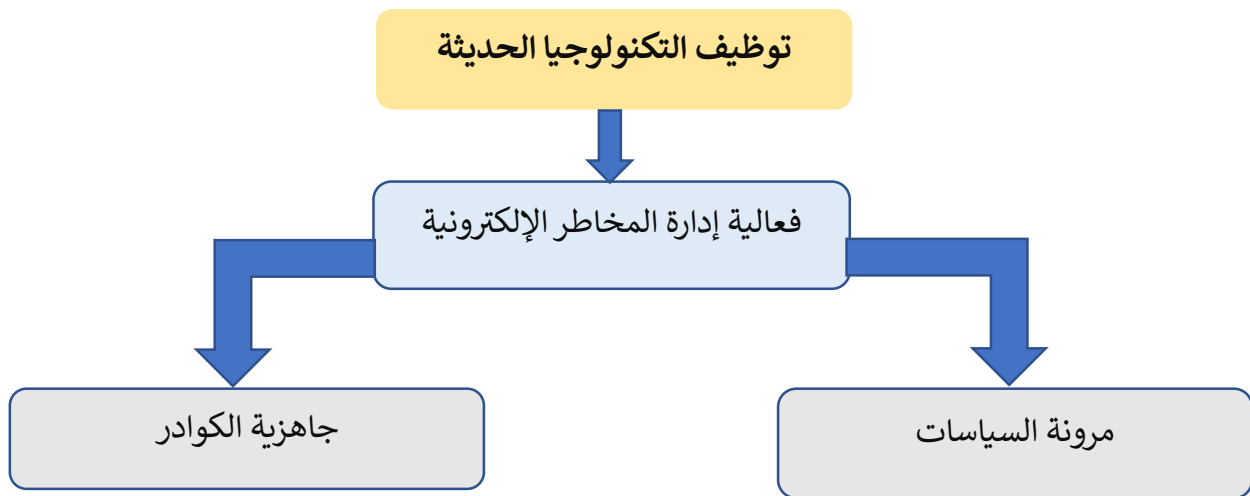
من خلال هذه الفروض، أسعى في دراستي إلى اختبار الروابط بين المتغيرات المستقلة المتعلقة باستخدام التكنولوجيا الحديثة، والمتغيرات التابعة المرتبطة بفعالية إدارة المخاطر الإلكترونية، بما يوفر أساسًا علميًا للخروج بتوصيات عملية قابلة للتطبيق.

6.1 نموذج الدراسة

بناءً على أهداف وتساؤلات وفروض الدراسة التي وضعتها، أسعى في هذه الدراسة لتقديم نموذج مفاهيمي يوضح العلاقة بين استخدام التكنولوجيا الحديثة بمختلف صورها (مثل الذكاء الاصطناعي وتحليلات البيانات الضخمة) وبين فعالية إدارة المخاطر الإلكترونية في المؤسسات السعودية والعربية.

يرتكز هذا النموذج على فكرة رئيسية مؤداها أن **توظيف التكنولوجيا الحديثة** يمثل المتغير المستقل الأساسي في الدراسة، بينما تمثل **فاعلية إدارة المخاطر الإلكترونية** المتغير التابع الذي أسعى لقياسه وتحليله. كما أرى أن هناك متغيرات وسيطة تؤثر على قوة العلاقة بين المتغيرين الأساسيين، وأبرزها :

- جاهزية الكوادر البشرية ومرونة السياسات والإجراءات الأمنية.
- وصف مكونات نموذج الدراسة
 - **المتغير المستقل:**
 - مستوى توظيف التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية.
 - يشمل استخدام الذكاء الاصطناعي، نظم إدارة معلومات الأمن (SIEM) ، وتحليلات البيانات التنبؤية.
 - **المتغير التابع:**
 - فعالية إدارة المخاطر الإلكترونية في المؤسسة.
 - يقاس من خلال سرعة اكتشاف التهديدات، تقليل الخسائر، ورفع جاهزية المؤسسة.
 - **المتغيرات الوسيطة:**
 - كفاءة الكوادر البشرية المؤهلة للتعامل مع التكنولوجيا الحديثة.
 - مرونة ووضوح السياسات الأمنية الداخلية.



الشكل (1)

العنصر	التوصيف
المتغير المستقل	توظيف التكنولوجيا الحديثة.
المتغير التابع	فاعلية إدارة المخاطر الإلكترونية.
المتغيرات الوسيطة	جاهزية الكوادر البشرية، مرونة السياسات الأمنية.

جدول 5: وصف عناصر نموذج الدراسة

من خلال هذا النموذج، أطمح إلى اختبار الفرضيات المتعلقة بالعلاقات بين هذه المتغيرات بشكل علمي ومنهجي، بما يتيح الخروج بنتائج دقيقة وقابلة للتطبيق في بيئة المؤسسات السعودية والعربية.

7.1 الدراسات السابقة

في سياق إعداد هذه الدراسة، حرصت على الاطلاع على مجموعة من الدراسات السابقة التي تناولت موضوع إدارة المخاطر الإلكترونية واستخدام التكنولوجيا الحديثة، بهدف الاستفادة من نتائجها في بناء إطار نظري متين. أسرد فيما يلي أهم الدراسات التي اطلعت عليها:

● الدراسة الأولى (Capgemini (2019 :

- اسم الدراسة: Reinventing Cybersecurity with Artificial Intelligence
- هدف الدراسة: استكشاف دور الذكاء الاصطناعي في تحسين فعالية الأمن السيبراني في المؤسسات الكبرى.
- أهم النتائج: أوضحت أن استخدام الذكاء الاصطناعي ساعد المؤسسات على تقليل زمن اكتشاف الهجمات بنسبة تصل إلى 60%، وخفض عدد الإنذارات الكاذبة بشكل كبير.
- المشكلات التي واجهها الباحث: صعوبة إقناع بعض الشركات بالإفصاح عن البيانات الأمنية الخاصة بها، إضافة إلى تحديات متعلقة بتنوع أنظمة الحماية المستخدمة بين المؤسسات.

● الدراسة الثانية: الغامدي (2022)

- اسم الدراسة: تحديات تطبيق الذكاء الاصطناعي في أمن المعلومات بالسعودية
- هدف الدراسة: تحديد العقبات التي تواجه المؤسسات السعودية في تبني تقنيات الذكاء الاصطناعي لحماية بياناتها.
- أهم النتائج: كشفت أن ضعف تدريب الكوادر البشرية ونقص الكفاءات المتخصصة أبرز المعوقات أمام توظيف الذكاء الاصطناعي بفعالية.
- المشكلات التي واجهها الباحث: انخفاض مستوى التعاون من بعض المؤسسات في تزويد الباحث بالمعلومات اللازمة، وصعوبة الحصول على بيانات دقيقة حول الاختراقات الأمنية.

● الدراسة الثالثة (2021) ENISA :

- اسم الدراسة: ENISA Threat Landscape 2021 :
- هدف الدراسة: تحليل أبرز التهديدات السيبرانية في أوروبا والعالم، وتقديم توصيات لتعزيز الأمن السيبراني في المؤسسات.
- أهم النتائج: بينت الدراسة ارتفاعاً ملحوظاً في هجمات الفدية، ودعت إلى الاستثمار في الحلول الاستباقية للكشف المبكر والاستجابة الفورية للهجمات.
- المشكلات التي واجهها الباحث: الحاجة المستمرة لتحديث البيانات بسبب سرعة تطور الهجمات الإلكترونية، مما تطلب وقتاً إضافياً للتحقق من دقة النتائج.

● الدراسة الرابعة: آل هلال (2021)

- اسم الدراسة: إدارة المخاطر الإلكترونية في المؤسسات السعودية: الواقع والتحديات
- هدف الدراسة: دراسة مدى تطبيق استراتيجيات إدارة المخاطر الإلكترونية في الشركات السعودية الصغيرة والمتوسطة.
- أهم النتائج: كشفت أن نسبة كبيرة من هذه الشركات لا تعتمد استراتيجيات واضحة لإدارة المخاطر، وتكتفي بحلول جزئية لا توفر حماية شاملة.
- المشكلات التي واجهها الباحث: صعوبة الوصول إلى صناع القرار في بعض الشركات لجمع البيانات الميدانية، وغياب دراسات سابقة محلية تساعد في بناء الإطار النظري.

أبرز المشكلات	النتائج الرئيسية	الهدف	اسم الدراسة
نقص تعاون الشركات الكبرى	تقليل زمن الاكتشاف وخفض الإنذارات الكاذبة	دور الذكاء الاصطناعي في الأمن السيبراني	Capgemini (2019)
صعوبة جمع بيانات دقيقة	ضعف تدريب الكوادر عائق رئيسي	تحديات الذكاء الاصطناعي في السعودية	الغامدي (2022)
ضرورة تحديث البيانات باستمرار	زيادة هجمات الفدية والحاجة للكشف المبكر	تحليل التهديدات السيبرانية عالمياً	ENISA (2021)
صعوبة الوصول للمسؤولين	غياب استراتيجيات واضحة في الشركات الصغيرة	إدارة المخاطر الإلكترونية في السعودية	آل هلال (2021)

جدول 6: مقارنة بين الدراسات السابقة

من خلال استعراض هذه الدراسات نجد أن هناك فجوة واضحة في الدراسات التي تربط بين التكنولوجيا الحديثة وإدارة المخاطر الإلكترونية في سياق البيئة السعودية والعربية، خاصة فيما يخص تصميم نماذج تطبيقية مخصصة. وهذا ما تسعى دراستي الحالية لسده من خلال تقديم إطار تطبيقي مبني على نتائج ميدانية حديثة.

8.1 المنطلقات النظرية للدراسة

تستند هذه الدراسة إلى مجموعة من الأطر والنظريات العلمية التي أرى أنها تمثل قاعدة أساسية لفهم طبيعة العلاقة بين توظيف التكنولوجيا الحديثة وفعالية إدارة المخاطر الإلكترونية في المؤسسات. ويشمل ذلك:

(1) نظرية إدارة المخاطر: (Risk Management Theory)

تنص هذه النظرية على أن عملية إدارة المخاطر تتكون من مراحل أساسية تبدأ بالتعرف على المخاطر وتحليلها وتقييمها، ثم وضع استراتيجيات للحد منها أو تجنبها، وأخيراً مراقبتها بشكل مستمر. أرى أن توظيف التكنولوجيا الحديثة، مثل الذكاء الاصطناعي، في كل مرحلة من هذه المراحل يساهم في تحسين القدرة على التعامل مع المخاطر الإلكترونية وتقليل آثارها المحتملة.

(2) نظرية الدفاع المتعدد الطبقات: (Defense in Depth)

تعتمد هذه النظرية على مفهوم أساسي هو بناء مستويات متعددة من الحماية على المستويات التقنية والتنظيمية والبشرية. أرى أن هذه النظرية مهمة جداً في دراستي، لأنها توضح ضرورة عدم الاكتفاء بحلول تقنية منفردة، بل بدمج تقنيات مثل نظم إدارة معلومات الأمن (SIEM) مع تدريب الكوادر والسياسات الأمنية المرنة لتحقيق حماية متكاملة.

(3) نظرية الذكاء الاصطناعي في الأمن السيبراني: (AI in Cybersecurity)

تفترض هذه النظرية أن تطبيق الذكاء الاصطناعي يساهم في تحسين سرعة ودقة الكشف عن التهديدات الإلكترونية، من خلال تدريب الأنظمة الذكية على بيانات تاريخية وتحليل الأنماط المشبوهة بشكل مستمر. وأرى في هذه النظرية حجر الأساس لإثبات أهمية التقنيات الحديثة في الدراسة الحالية.

(4) نظرية الوعي الأمني: (Security Awareness)

تؤكد هذه النظرية أن العامل البشري هو العنصر الأضعف في سلسلة الحماية السيبرانية، وأن رفع مستوى الوعي الأمني والتدريب المستمر للعاملين في المؤسسات يعد جزءاً أساسياً لضمان فعالية أي تقنية أمنية حديثة. لذلك أعتبر هذه النظرية جوهرية لدعم فرضيات دراستي المتعلقة بأهمية تأهيل الكوادر البشرية.

النظرية / الإطار	دورها في الدراسة
نظرية إدارة المخاطر	توضح مراحل التعامل مع المخاطر الإلكترونية.
نظرية الدفاع المتعدد الطبقات	تبرز أهمية تكامل الحلول التقنية والسياسات والإجراءات.
نظرية الذكاء الاصطناعي للأمن	تفسر كيفية تحسين قدرات الكشف المبكر للتهديدات.
نظرية الوعي الأمني	تركز على أهمية العامل البشري في نجاح استراتيجيات الحماية.

جدول 7: المنطلقات النظرية ودورها في الدراسة

من خلال هذه المنطلقات، أهدف إلى بناء إطار نظري متكامل يساعدني على تحليل العلاقة بين المتغيرات الرئيسية في دراستي، بما يضمن الوصول إلى نتائج دقيقة وقابلة للتطبيق في الواقع العملي للمؤسسات السعودية والعربية.

9.1 المنهجية وطرق البحث

أسعى في دراستي هذه إلى اتباع منهجية علمية دقيقة تجمع بين المنهج الوصفي التحليلي والمنهج التطبيقي؛ بهدف تحقيق أقصى قدر ممكن من الدقة والعمق في تحليل البيانات والوصول إلى نتائج موثوقة تسهم في تطوير الممارسات الحالية لإدارة المخاطر الإلكترونية.

(1) نوع المنهج:

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي، الذي أرى أنه الأنسب لوصف الواقع الحالي لإدارة المخاطر الإلكترونية في المؤسسات السعودية والعربية، وتحليل العلاقة بين توظيف التكنولوجيا الحديثة وفعالية هذه الإدارة. كما يوظف المنهج التطبيقي في تصميم نموذج عملي بناءً على نتائج الدراسة الميدانية.

(2) مجتمع وعينة الدراسة:

يتكون مجتمع الدراسة من موظفي أقسام تقنية المعلومات والأمن السيبراني في المؤسسات السعودية والعربية، بما يشمل قطاعات مختلفة مثل الاتصالات، والخدمات المالية، والرعاية الصحية، نظرًا لحساسيتها العالية وخطورة استهدافها بالهجمات الإلكترونية. وأسعى إلى اختيار عينة عشوائية طبقية لضمان تمثيل جميع أحجام المؤسسات (كبيرة، متوسطة، صغيرة) في الدراسة.

(3) أدوات جمع البيانات:

(4) الاستبانة الإلكترونية:

صممت استبانة شاملة تضم أسئلة مغلقة وفق مقياس ليكرت الخماسي، إضافة إلى أسئلة مفتوحة، بهدف جمع بيانات كمية ونوعية في آن واحد.

(5) دليل المقابلات شبه المقتنة:

أستخدمه لإجراء مقابلات مع مسؤولي أقسام الأمن السيبراني في المؤسسات، بهدف فهم سياساتهم وتجاربهم في توظيف التكنولوجيا الحديثة.

إجراءات جمع البيانات:

يتم توزيع الاستبانات إلكترونياً عبر البريد الرسمي للمؤسسات، مرفقة بخطاب رسمي يوضح أهداف الدراسة ويؤكد سرية البيانات. كما ترتب مواعيد المقابلات الهاتفية أو المباشرة بالتنسيق مع المسؤولين في المؤسسات المستهدفة.

10.1 طرق تحليل البيانات:

- التحليل الوصفي باستخدام المتوسطات الحسابية والانحرافات المعيارية لوصف خصائص العينة.
- التحليل الاستدلالي باستخدام اختبارات T-Test و ANOVA لاختبار فروض الدراسة.
- تحليل الارتباط باستخدام معامل بيرسون لقياس قوة العلاقة بين المتغيرات.
- تحليل المحتوى النوعي لاستخلاص الأنماط المتكررة في إجابات الأسئلة المفتوحة والمقابلات

المرحلة	الإجراء
تصميم أدوات البحث	إعداد الاستبانة ودليل المقابلات
جمع البيانات	توزيع الاستبانات وإجراء المقابلات
معالجة البيانات	الترميز والتحليل الإحصائي والنوعي
كتابة النتائج	تفسير المعطيات وصياغة الاستنتاجات

جدول 8: مراحل تنفيذ الدراسة

من خلال هذه المنهجية، أطمح إلى الوصول إلى نتائج علمية دقيقة وشاملة تساعد في بناء نموذج تطبيقي يساهم في تحسين قدرة المؤسسات على إدارة المخاطر الإلكترونية باستخدام التكنولوجيا الحديثة بشكل فعال وعملي.

11.1 مصادر البيانات

تسعى هذه الدراسة إلى الاعتماد على نوعين رئيسيين من البيانات بهدف ضمان شمولية التحليل ودقة النتائج التي أصل إليها:

1. البيانات الأولية: (Primary Data)

أرى أنها تمثل العمود الفقري للدراسة، حيث أجمعها بنفسني من خلال الاستبانات الإلكترونية والمقابلات شبه المقننة مع موظفي أقسام تقنية المعلومات والأمن السيبراني في المؤسسات المستهدفة. تهدف هذه البيانات إلى وصف الواقع الفعلي لإدارة المخاطر الإلكترونية وقياس مدى توظيف التكنولوجيا الحديثة.

2. البيانات الثانوية: (Secondary Data)

وتشمل الدراسات السابقة، الكتب والمراجع العلمية، والتقارير الحكومية والدولية مثل تقارير ENISA والهيئة الوطنية للأمن السيبراني. أرى أن هذه المصادر أساسية لبناء الإطار النظري للدراسة، ولإثراء التحليل بمقارنتها مع النتائج الميدانية.

نوع البيانات	أمثلة على المصادر	دورها في الدراسة
أولية	استبانات، مقابلات	جمع معلومات ميدانية مباشرة ودقيقة
ثانوية	دراسات سابقة، تقارير ENISA وهيئة الأمن	بناء الإطار النظري وتفسير النتائج

جدول 9: مصادر البيانات وأهمية كل منها

12.1 أدوات الدراسة

لتحقيق أهداف الدراسة والوصول إلى بيانات دقيقة وموثوقة، قمت بإعداد الأدوات التالية:

1. الاستبانة الإلكترونية:

صممت لتضم ثلاثة محاور رئيسية:

- المحور الأول: البيانات الديموغرافية للمشاركين (مثل المنصب الوظيفي، سنوات الخبرة، حجم المؤسسة).
 - المحور الثاني: مستوى توظيف التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية.
 - المحور الثالث: أبرز التحديات التي تواجه المؤسسات في تبني الحلول التقنية.
- استخدمت في الاستبانة أسئلة مغلقة بنظام ليكرت الخماسي (من 1=لا أوافق بشدة إلى 5=أوافق بشدة) لقياس درجة الموافقة على العبارات.

2. دليل المقابلات شبه المقتنة:

وضعت دليلاً يتضمن أسئلة مفتوحة موجهة لمسؤولي الأمن السيبراني في المؤسسات الكبرى، بهدف جمع بيانات نوعية معمقة حول سياسات حماية المعلومات، ومدى توافقها مع التهديدات المتجددة.

3. نظام إدارة الاستبانات الإلكترونية:

قررت استخدام منصة مثل Google Forms أو SurveyMonkey لتوزيع الاستبانات إلكترونياً، بما يضمن سهولة الوصول للمشاركين وسرية إجاباتهم.

الأداة	الفئة المستهدفة	الهدف منها
الاستبانة الإلكترونية	موظفو تقنية المعلومات والأمن	جمع بيانات كمية عن توظيف التقنية والتحديات
دليل المقابلات	مسؤولو الأمن السيبراني	جمع بيانات نوعية عن السياسات والخبرات
منصة إدارة الاستبانات	جميع المشاركين	توزيع الاستبانات وتحليل الإجابات بسهولة

جدول 11: أدوات الدراسة واستخداماتها

من خلال هذه الأدوات، أسعى إلى بناء قاعدة بيانات شاملة تمكّني من الإجابة عن تساؤلات الدراسة واختبار فروضها بشكل علمي دقيق.

• الأساليب الإحصائية المستخدمة

أسعى في دراستي هذه إلى استخدام مجموعة من الأساليب الإحصائية المناسبة لطبيعة البيانات التي سأجمعها، وذلك لضمان تحليلها بدقة والوصول إلى نتائج علمية موثوقة. وأعتمد في ذلك على:

● التحليل الوصفي: (Descriptive Statistics)

أستخدمه لحساب التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية، بهدف وصف خصائص مجتمع الدراسة وبيان درجة موافقتهم على بنود الاستبانة.

● التحليل الاستدلالي: (Inferential Statistics)

○ اختبار T-Test للعينات المستقلة لقياس الفروق ذات الدلالة الإحصائية بين المجموعات، مثل المؤسسات التي تعتمد التكنولوجيا الحديثة وتلك التي لا تعتمد.

○ أطبق تحليل التباين الأحادي (One-way ANOVA) عند الحاجة لدراسة الفروق بناءً على متغيرات ديموغرافية مثل حجم المؤسسة أو سنوات الخبرة.

○ تحليل الارتباط: (Correlation Analysis)

أسعى لقياس قوة العلاقة بين المتغيرات المستقلة (مثل مستوى توظيف التكنولوجيا) والمتغير التابع (فعالية إدارة المخاطر الإلكترونية)، باستخدام معامل ارتباط بيرسون.

● تحليل المحتوى النوعي: (Qualitative Content Analysis)

لتحليل إجابات الأسئلة المفتوحة في الاستبانات ونصوص المقابلات، واستخلاص الأنماط المتكررة التي تساعد في تفسير النتائج الكمية ودعمها.

الأسلوب الإحصائي	الغرض منه
التحليل الوصفي	وصف خصائص مجتمع الدراسة
اختبار T-Test	اختبار فروق بين المجموعات
تحليل التباين ANOVA	دراسة تأثير المتغيرات الديموغرافية
تحليل الارتباط بيرسون	قياس قوة العلاقة بين المتغيرات
تحليل المحتوى النوعي	تفسير البيانات النوعية واستخلاص الأنماط

جدول 11: الأساليب الإحصائية المستخدمة وأغراضها

13.1 حدود الدراسة

لضمان دقة التفسير ووضوح النتائج التي أصل إليها، أرى ضرورة توضيح حدود هذه الدراسة كما يلي:

(1) الحدود الموضوعية:

تركز دراستي على العلاقة بين توظيف التكنولوجيا الحديثة وإدارة المخاطر الإلكترونية، ولا تتطرق لاستخدامات أخرى للتكنولوجيا مثل التسويق الرقمي أو إدارة الموارد البشرية.

(2) الحدود المكانية:

تقتصر الدراسة على المؤسسات السعودية وبعض المؤسسات الخليجية، مما قد يؤثر على إمكانية تعميم النتائج على بيانات أعمال في مناطق جغرافية مختلفة.

(3) الحدود الزمنية:

تمثل البيانات التي سأجمعها خلال الفترة من سبتمبر إلى نوفمبر 2025، وبالتالي فإن النتائج تعكس الواقع خلال هذه الفترة فقط، وقد تتغير مستقبلاً مع تطور التقنيات.

(4) الحدود البشرية:

تقتصر العينة على العاملين في أقسام تقنية المعلومات والأمن السيبراني داخل المؤسسات، دون إشراك العملاء أو مستخدمي الخدمات الخارجية، ما قد يحد من شمولية الرؤية لبعض الجوانب.

نوع الحد	وصفه	أثره المحتمل على النتائج
موضوعي	يركز على توظيف التكنولوجيا في إدارة المخاطر	لا يشمل استخدامات أخرى للتقنية
مكاني	مقتصر على السعودية وبعض دول الخليج	قد يحد من تعميم النتائج عالمياً
زمني	البيانات من فترة محددة في 2025	النتائج مرتبطة بظروف تلك الفترة
بشري	مقتصر على موظفي التقنية والأمن السيبراني	قد يغفل آراء المستخدمين الخارجيين

جدول 12: حدود الدراسة وتأثيرها المحتمل

الفصل الثاني: الإطار النظري

تمهيد

أسعى في هذا الفصل إلى تقديم إطار نظري متكامل يوضح الخلفية العلمية لموضوع دراستي حول توظيف التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية في المؤسسات السعودية والعربية. وقد جاء اهتمامي بهذا الإطار انطلاقاً من إدراكي بأن فهم المفاهيم الأساسية لإدارة المخاطر الإلكترونية من جهة، والإلمام بالتقنيات الحديثة في مجال الأمن السيبراني من جهة أخرى، يمثلان الأساس الذي تقوم عليه أي محاولة جادة لتطوير سياسات واستراتيجيات فعالة لحماية الأصول الرقمية في المؤسسات.

وفي ضوء ما شهدته بيئة الأعمال من تغيرات متسارعة بفعل التحول الرقمي وزيادة الاعتماد على الأنظمة الإلكترونية في مختلف العمليات التشغيلية، باتت المخاطر الإلكترونية تمثل تهديداً حقيقياً لاستمرارية الأعمال وسلامة البيانات. ومع أن إدارة المخاطر تعتبر من العلوم الإدارية القديمة نسبياً، إلا أن إدارة المخاطر الإلكترونية تحديداً تطورت بشكل ملحوظ خلال العقود الأخيرة، مدفوعة بظهور تهديدات سيبرانية متجددة تتطلب أدوات وتقنيات متقدمة للكشف عنها ومواجهتها.

كما أصبحت التكنولوجيا الحديثة مثل الذكاء الاصطناعي، وتقنيات التحليل السلوكي، وأنظمة إدارة معلومات الأمن (SIEM) تلعب دوراً محورياً في تطوير قدرات المؤسسات على التنبؤ بالتهديدات وتقليل آثارها، الأمر الذي دفعني في هذا الفصل إلى تخصيص مبحث أول لتأصيل المفاهيم المتعلقة بإدارة المخاطر الإلكترونية، ومبحث ثانٍ لتوضيح كيفية توظيف التكنولوجيا الحديثة في تحسين كفاءة هذه الإدارة.

ومن خلال هذا الإطار النظري، أسعى إلى بناء قاعدة معرفية علمية تتيح لي تحليل العلاقة بين المتغيرات الرئيسة في دراستي، والوصول إلى فهم عميق للأبعاد التي تؤثر في قدرة المؤسسات على حماية بياناتها وأصولها الرقمية بشكل فعال في ظل بيئة إلكترونية معقدة ومتغيرة باستمرار.

1.2 المبحث الأول: مفاهيم إدارة المخاطر الإلكترونية

1.1.2 مقدمة

انطلاقاً من قناعاتي بأن فهم المفاهيم الأساسية لإدارة المخاطر الإلكترونية يشكل الركيزة الأولى لبناء أي إطار عملي أو نظري في هذا المجال، أخصص هذا المبحث لتناول المفاهيم المتعلقة بالمخاطر الإلكترونية وإدارتها، من خلال استعراض تعريفاتها وأهميتها وأهدافها وأسباب بروزها كضرورة استراتيجية في المؤسسات المعاصرة.

لقد أدت الثورة الرقمية والانتشار الواسع للتكنولوجيا في شتى مجالات الحياة إلى ظهور أنواع جديدة من المخاطر لم تكن المؤسسات تواجهها في الماضي، مثل هجمات الفدية، والاختراقات واسعة النطاق، والتصيد الإلكتروني المتقدم، وهي تهديدات لا تقتصر آثارها على الجانب التقني فقط، بل قد تمتد إلى الإضرار بسمعة المؤسسة وتعطيل أعمالها والتسبب في خسائر مالية جسيمة. (ENISA, 2021)

وبما أن إدارة المخاطر الإلكترونية أصبحت جزءاً لا يتجزأ من الاستراتيجيات الإدارية في المؤسسات الكبرى والصغرى على حد سواء، أسعى في هذا المبحث إلى تناول التطور التاريخي لمفهوم إدارة المخاطر الإلكترونية،

وتوضيح تعريفاتها المختلفة في الأدبيات الحديثة، مع التركيز على الأبعاد الأساسية التي تقوم عليها، والتي تشمل على الأبعاد التقنية، البشرية، والتنظيمية.

كما أرى أن تسليط الضوء على أسباب تصاعد أهمية إدارة المخاطر الإلكترونية سيساعدني في توضيح الصورة الكاملة للقارئ، وسببين له لماذا أصبحت هذه الإدارة اليوم ضرورة ملحة لحماية أصول المؤسسات وضمان استمرارية أعمالها في بيئة عمل رقمية سريعة التغير.

2.1.2 التطور التاريخي لإدارة المخاطر الإلكترونية

في هذا الجزء نسعى إلى تتبع المراحل التاريخية التي مرت بها إدارة المخاطر الإلكترونية لفهم كيف تطورت من مجرد ممارسات أمنية بسيطة إلى أن أصبحت تخصصًا متكاملًا يعتمد على أحدث التقنيات والأنظمة.

في بدايات الاعتماد المؤسسي على الحواسيب في الستينيات والسبعينيات من القرن الماضي، كانت أغلب التهديدات الأمنية تتمثل في المخاطر المادية كسرقة الأجهزة أو فقدان البيانات بسبب أعطال فنية، وكان التعامل معها يتم من خلال إجراءات تقليدية مثل تأمين الغرف وحفظ النسخ الورقية. ومع بداية الثمانينيات والتسعينيات وظهرت شبكات الاتصال وانتشار استخدام الإنترنت، بدأت التهديدات تتحول إلى مخاطر إلكترونية مثل الفيروسات والبرمجيات الخبيثة التي تستهدف البيانات مباشرة، ما دفع المؤسسات إلى تطوير سياسات حماية رقمية محدودة النطاق.

ومع مطلع الألفية الثالثة، شهد العالم تسارعًا هائلًا في تطور الإنترنت وتقنيات الاتصالات، ترافق مع زيادة ملحوظة في الهجمات الإلكترونية المنظمة، مثل هجمات رفض الخدمة (DDoS) وبرمجيات الفدية، وهو ما أجبر المؤسسات والحكومات على تخصيص وحدات متخصصة في إدارة المخاطر الإلكترونية وتطوير أساليب الكشف المبكر والتصدي للتهديدات.

وفي العقد الأخير تحديدًا، ومع انتشار تطبيقات الحوسبة السحابية، وإنترنت الأشياء (IoT)، وتقنيات الذكاء الاصطناعي، أصبحت إدارة المخاطر الإلكترونية أكثر تعقيدًا وتشعبًا، ولم تعد تقتصر على إجراءات تقنية فقط، بل امتدت لتشمل تدريب الكوادر البشرية ووضع سياسات تنظيمية واستراتيجيات تكاملية بين مختلف أقسام المؤسسة.

ومن خلال هذا الاستعراض التاريخي، أرى أن إدارة المخاطر الإلكترونية تطورت من كونها جزءًا محدودًا من مهام أقسام تقنية المعلومات إلى أن أصبحت اليوم وظيفة استراتيجية أساسية تشارك فيها مختلف مستويات الإدارة في المؤسسات المعاصرة.

3.1.2 تعريف المخاطر الإلكترونية

في سياق هذه الدراسة، أرى أن تحديد مفهوم واضح ودقيق للمخاطر الإلكترونية يمثل خطوة أساسية لفهم طبيعة التهديدات التي تواجه المؤسسات في العصر الرقمي، ويساعد في بناء استراتيجية فعالة لإدارتها. وقد تناولت الأدبيات مصطلح المخاطر الإلكترونية (Cyber Risks) بتعريفات متعددة، لكنها تتفق في جوهرها على أنها جميع التهديدات المحتملة التي قد تؤدي إلى الإضرار بالأنظمة الإلكترونية أو البيانات أو الاتصالات الرقمية للمؤسسة، سواء كانت هذه التهديدات ناتجة عن هجمات متعمدة أو عن أخطاء بشرية أو أعطال فنية. (Von Solms & Van Niekerk, 2013)

ويشمل هذا المفهوم المخاطر المتعلقة بفقدان سرية المعلومات Confidentiality ، أو اختراق سلامتها Integrity ، أو التأثير على إتاحتها Availability ، وهي العناصر الثلاثة الجوهرية في أمن المعلومات المعروفة بنموذج CIA (CIA Triad) (Sharma & Sahay, 2021).

كما تتضمن المخاطر الإلكترونية المخاطر الناتجة عن الاستخدام السيء للأنظمة من قبل الموظفين، أو استغلال الثغرات الأمنية في البرمجيات والشبكات، إضافة إلى مخاطر الهندسة الاجتماعية التي تعتمد على خداع الأفراد للحصول على معلومات حساسة.

وبناءً على ما سبق، أعرّف المخاطر الإلكترونية في دراستي بأنها:

“مجموعة التهديدات الرقمية المحتملة التي قد تؤثر سلباً على سرية البيانات أو سلامتها أو إتاحتها، نتيجة هجمات إلكترونية متعمدة أو أخطاء بشرية أو أعطال تقنية، وما قد يترتب عليها من خسائر مالية أو تشغيلية أو سمعة للمؤسسة”.

4.1.2 تعريف إدارة المخاطر الإلكترونية

أرى أن إدارة المخاطر الإلكترونية (Cyber Risk Management) تمثل الإطار المنهجي الذي تعتمد عليه المؤسسات في التعامل مع المخاطر الرقمية المحتملة التي قد تهدد أنظمتها وبياناتها. وتُعرف إدارة المخاطر الإلكترونية في الأدبيات بأنها:

“عملية مستمرة ومنهجية لتحديد المخاطر الإلكترونية، وتقييمها، وتصنيفها، ووضع وتنفيذ السياسات والإجراءات اللازمة للحد منها أو تجنبها أو التعامل معها، بهدف حماية أصول المؤسسة الرقمية وضمان استمرارية أعمالها” (ENISA, 2021).

وتقوم إدارة المخاطر الإلكترونية على عدة خطوات أساسية:

- ❖ **التعرف على المخاطر:** من خلال تحديد مصادر التهديدات ونقاط الضعف في البنية التحتية الرقمية للمؤسسة.
- ❖ **تحليل المخاطر:** لتقييم احتمال وقوع كل خطر وتأثيره المحتمل على العمليات التشغيلية والمالية.
- ❖ **تقييم المخاطر:** بتحديد مستوى الخطر (مرتفع، متوسط، منخفض) ووضع أولويات المعالجة.
- ❖ **معالجة المخاطر:** عبر اختيار استراتيجية مناسبة مثل تجنب الخطر أو تقبله أو نقله (بالتأمين) أو تخفيفه باستخدام الحلول التقنية والإجراءات التنظيمية.
- ❖ **المتابعة والمراجعة:** بمراقبة فاعلية التدابير المتخذة وإعادة تقييم المخاطر بشكل دوري في ضوء التغيرات التكنولوجية وظهور تهديدات جديدة.

ومن خلال هذا التعريف، أرى أن إدارة المخاطر الإلكترونية لم تعد مجرد وظيفة تقنية تابعة لقسم تقنية المعلومات، بل أصبحت جزءاً استراتيجياً من منظومة إدارة المخاطر المؤسسية ككل، تتطلب تكاملاً بين مختلف الإدارات لضمان حماية متكاملة للأصول الرقمية.

5.1.2 أهمية إدارة المخاطر الإلكترونية في المؤسسات الحديثة

أن إدارة المخاطر الإلكترونية أصبحت اليوم ضرورة استراتيجية لا غنى عنها في المؤسسات الحديثة، نظراً للتغيرات الهائلة التي فرضها التحول الرقمي على طبيعة الأعمال والبيئة التنافسية. فقد أدى الاعتماد المتزايد على الأنظمة

الإلكترونية والبنى التحتية الرقمية إلى توسيع مساحة التعرض للتهديدات الإلكترونية، وهو ما جعل أي اختراق محتمل قادرًا على التسبب في خسائر كبيرة قد تهدد بقاء المؤسسة نفسها في السوق. (Bada et al., 2019) وتتجلى أهمية إدارة المخاطر الإلكترونية فيما يلي:

❖ **حماية الأصول الرقمية:** مثل قواعد البيانات، البرمجيات، والبنى التحتية للشبكات، والتي تعتبر من أهم أصول المؤسسات في العصر الرقمي.

❖ **ضمان استمرارية الأعمال:** إذ يساهم التخطيط المسبق لإدارة المخاطر في تقليل أوقات التوقف الناتجة عن الهجمات الإلكترونية، مما يضمن استمرار تقديم الخدمات دون انقطاع.

❖ **الامتثال للأنظمة والتشريعات:** حيث تلزم الكثير من الدول والمنظمات المؤسسات بتطبيق سياسات صارمة لحماية البيانات الشخصية والمالية، وإلا تعرضت لغرامات أو عقوبات قانونية.

❖ **حماية السمعة المؤسسية:** في ظل سرعة انتشار الأخبار على الإنترنت ووسائل التواصل الاجتماعي، يمكن لأي حادثة اختراق أن تضر بسمعة المؤسسة بشكل يصعب استعادته دون وجود استراتيجيات فعالة لإدارة المخاطر الإلكترونية.

❖ **تعزيز الثقة مع العملاء والشركاء:** إذ يساهم إثبات التزام المؤسسة بتطبيق أفضل ممارسات الحماية الإلكترونية في بناء الثقة، مما يعزز علاقاتها التجارية ويمنحها ميزة تنافسية.

❖ **خفض التكاليف الناتجة عن الهجمات:** حيث يساعد التخطيط الجيد لإدارة المخاطر الإلكترونية في تقليل الخسائر المباشرة وغير المباشرة المرتبطة بالاختراقات، بما في ذلك تكاليف الاستجابة للحوادث وتعويض المتضررين.

وبناءً على ذلك، فإن إدارة المخاطر الإلكترونية لم تعد مجرد خيار للمؤسسات الحديثة، بل أصبحت مطلبًا أساسيًا لاستدامة أعمالها وحمايتها في بيئة مليئة بالتهديدات الرقمية المتطورة.

6.1.2 أهداف إدارة المخاطر الإلكترونية

أرى أن إدارة المخاطر الإلكترونية لا تقتصر على كونها نشاطًا وقائيًا فقط، بل هي عملية استراتيجية تهدف إلى تمكين المؤسسة من مواجهة التهديدات المتجددة بكفاءة واستباقية. وتتعدد الأهداف التي تسعى المؤسسات لتحقيقها من خلال إدارة المخاطر الإلكترونية، ومن أبرزها:

(1) **حماية سرية المعلومات: (Confidentiality)** وذلك بمنع الوصول غير المصرح به إلى البيانات الحساسة، سواء كانت بيانات مالية أو معلومات خاصة بالعملاء أو أسرار تجارية.

(2) **الحفاظ على سلامة البيانات: (Integrity)** لضمان عدم التلاعب أو التعديل غير المصرح به في البيانات أثناء تخزينها أو نقلها عبر الشبكات.

(3) **ضمان إتاحة الأنظمة والخدمات: (Availability)** من خلال التأكد من أن الأنظمة الإلكترونية تعمل بشكل مستمر دون انقطاع، وتقليل أوقات التوقف الناتجة عن الهجمات الإلكترونية أو الأعطال الفنية.

- (4) الحد من الخسائر المالية: بتقليل التكاليف المباشرة وغير المباشرة الناجمة عن الحوادث الأمنية مثل الغرامات والعقوبات والإصلاحات الفنية وفقدان العملاء.
- (5) تحقيق الامتثال التشريعي والتنظيمي: وذلك بالتوافق مع القوانين الوطنية والدولية المتعلقة بأمن المعلومات وحماية البيانات، مثل لائحة حماية البيانات الأوروبية (GDPR) أو الأنظمة المحلية مثل سياسة الأمن السيبراني في المملكة العربية السعودية.
- (6) تعزيز الثقة المؤسسية: حيث تهدف إدارة المخاطر الإلكترونية إلى إثبات التزام المؤسسة بأعلى معايير الأمان، بما يعزز الثقة لدى العملاء والشركاء ويمنح المؤسسة ميزة تنافسية في السوق.
- (7) دعم استمرارية الأعمال: بوضع خطط للطوارئ وخطط استعادة البيانات بعد الكوارث (Disaster Recovery Plans) لضمان سرعة استئناف الأعمال وتقليل أثر الهجمات على العمليات التشغيلية.
- من خلال تحقيق هذه الأهداف، أسعى في دراستي لتبسيط الضوء على أهمية دمج إدارة المخاطر الإلكترونية ضمن الاستراتيجيات المؤسسية الكبرى، وليس الاكتفاء بمعالجتها كإجراءات تقنية معزولة عن الإدارة العليا.
- 7.1.2 أسباب تزايد الحاجة لإدارة المخاطر الإلكترونية في العصر الرقمي
- انطلاقاً من متابعتي لتطور بيئة الأعمال الرقمية، أرى أن هناك عدة أسباب رئيسية أسهمت في تصاعد أهمية إدارة المخاطر الإلكترونية في المؤسسات الحديثة، ومنها:
- (1) التوسع في التحول الرقمي: حيث أدى الاعتماد المتزايد على الأنظمة الإلكترونية والحوسبة السحابية والخدمات الرقمية إلى اتساع مساحة التعرض للتهديدات الإلكترونية بشكل غير مسبوق.
 - (2) زيادة تعقيد الهجمات السيبرانية: فقد أصبحت الهجمات الإلكترونية أكثر تطوراً وابتكاراً، مثل هجمات الفدية الموجهة (Targeted Ransomware) وهجمات سلاسل التوريد (Supply Chain Attacks)، التي تستهدف عدة أطراف في وقت واحد.
 - (3) الاعتماد على أطراف خارجية: (Third Parties) إذ تعتمد المؤسسات الحديثة بشكل كبير على مزودي خدمات التكنولوجيا والحوسبة السحابية، ما يزيد من احتمالية التعرض لمخاطر ناتجة عن ضعف أمان هذه الأطراف.
 - (4) ظهور تشريعات صارمة لحماية البيانات: مثل النظام الأوروبي العام لحماية البيانات (GDPR) والقوانين المحلية، التي تلزم المؤسسات بحماية معلومات عملائها، وإلا تعرضت لغرامات مالية ضخمة قد تهدد استمراريته.
 - (5) التوسع في العمل عن بُعد: الذي أصبح واقعاً في العديد من المؤسسات بعد جائحة كوفيد-19، ما زاد من التحديات الأمنية الناتجة عن استخدام شبكات وإنترنت منزلية قد لا تكون آمنة بما يكفي.
 - (6) تعدد الأجهزة والأنظمة المتصلة: مع انتشار إنترنت الأشياء (IoT) أصبحت المؤسسات تدير عددًا هائلاً من الأجهزة المتصلة بالشبكة، ما يرفع من فرص استغلال الثغرات الأمنية في هذه الأجهزة.
 - (7) الحاجة لحماية السمعة المؤسسية: في عصر الإعلام الرقمي وانتشار الأخبار بسرعة فائقة، يمكن لأي حادثة اختراق أن تتسبب بأضرار جسيمة لسمعة المؤسسة، مما يجعل إدارة المخاطر الإلكترونية ضرورة لحماية الثقة مع العملاء والشركاء.

ومن خلال ما سبق، أرى أن هذه الأسباب مجتمعة جعلت إدارة المخاطر الإلكترونية تتحول من كونها خيارًا تقنيًا إلى ضرورة استراتيجية لا بد منها لضمان استمرار الأعمال وحماية المصالح المؤسسية في ظل البيئة الرقمية المتغيرة والمتسارعة.

8.1.2 أبعاد إدارة المخاطر الإلكترونية

في هذا الجزء نسعى إلى توضيح الأبعاد الأساسية التي تقوم عليها إدارة المخاطر الإلكترونية في المؤسسات الحديثة، إذ أرى أن فعالية هذه الإدارة لا تتحقق إلا عند مراعاة الأبعاد التالية بشكل متكامل:

❖ البعد التقني:

يتمثل في اعتماد أحدث الحلول التقنية للكشف المبكر عن التهديدات، مثل أنظمة إدارة معلومات الأمن والأحداث (SIEM)، حلول كشف البرمجيات الخبيثة، والجدران النارية المتطورة. كما يشمل هذا البعد تأمين البنية التحتية الرقمية، وتطبيق سياسات تحديث وصيانة دورية للأنظمة لسد الثغرات الأمنية.

❖ البعد البشري:

يعتبر البعد البشري حجر الزاوية في أي استراتيجية ناجحة لإدارة المخاطر الإلكترونية، حيث تشير الدراسات إلى أن العنصر البشري يمثل أضعف حلقة في سلسلة الحماية. لذلك فإن رفع مستوى الوعي الأمني لدى الموظفين وتدريبهم على اكتشاف محاولات الاحتيال والالتزام بسياسات الأمان الرقمية أمر بالغ الأهمية.

❖ البعد التنظيمي:

يتعلق بوضع السياسات والإجراءات الواضحة التي تنظم التعامل مع المخاطر الإلكترونية، مثل خطة إدارة الأزمات وخطط استمرارية الأعمال وخطط استعادة البيانات بعد الكوارث (Disaster Recovery Plans). كما يشمل تحديد الأدوار والمسؤوليات بين الإدارات المختلفة فيما يخص الأمن السيبراني.

❖ البعد القانوني والتشريعي:

يتعلق بالتزام المؤسسة بالتشريعات والقوانين المحلية والدولية المنظمة لحماية البيانات وأمن المعلومات. أرى أن الإلمام بهذا البعد وتطبيقه يساعد المؤسسة على تجنب العقوبات والغرامات ويحميها من المخاطر القانونية المترتبة على حوادث الاختراق.

❖ البعد المالي:

ويشمل رصد الميزانيات الكافية لتنفيذ استراتيجيات إدارة المخاطر الإلكترونية، إذ إن نقص الموارد المالية يعد من أكبر العوائق أمام تطبيق حلول الحماية المتقدمة.

البُعد	التوضيح
التقني	تأمين الأنظمة باستخدام الحلول البرمجية والأجهزة الحديثة
البشري	تدريب الموظفين وتعزيز وعيهم الأمني
التنظيمي	وضع السياسات والإجراءات وإدارة الأزمات

البُعد	التوضيح
القانوني والتشريعي	الالتزام بالتشريعات المحلية والدولية لحماية البيانات
المالي	تخصيص الموارد المالية الكافية لتطبيق استراتيجيات الحماية

جدول 13: أبعاد إدارة المخاطر الإلكترونية

من خلال هذه الأبعاد، يتضح أن إدارة المخاطر الإلكترونية تتحول إلى منظومة متكاملة تضمن الحماية الفاعلة للمؤسسة، بدلاً من الاقتصاد على حلول تقنية منفردة لا تغطي جميع جوانب الخطر.

2.2 المبحث الثاني: التكنولوجيا الحديثة ودورها في إدارة المخاطر الإلكترونية

1.2.2 مقدمة

انطلاقاً من إدراكي العميق بأن التهديدات الإلكترونية تتطور بوتيرة متسارعة لا يمكن مواجهتها بالأساليب التقليدية وحدها، أرى أن توظيف التكنولوجيا الحديثة أصبح الخيار الاستراتيجي الوحيد للمؤسسات الراغبة في حماية أصولها الرقمية بشكل فعال. فقد ساهمت الابتكارات التقنية في توفير حلول متقدمة قادرة على الكشف المبكر عن التهديدات وتحليلها والتصدي لها بسرعة فائقة، بما يتجاوز القدرات البشرية المحدودة في التعامل مع حجم وسرعة الهجمات الإلكترونية الحالية. (Sharma & Sahay, 2021)

لقد لاحظت من خلال متابعتي للدراسات الحديثة أن التقنيات الجديدة مثل الذكاء الاصطناعي، تعلم الآلة (Machine Learning)، تحليلات البيانات الضخمة (Big Data Analytics)، وتقنيات البلوك تشين (Blockchain)، لعبت دوراً جوهرياً في إعادة تشكيل مفهوم إدارة المخاطر الإلكترونية من نموذج تفاعلي يعتمد على الاستجابة بعد وقوع الحوادث إلى نموذج استباقي قائم على التنبؤ بالتهديدات وتقليل فرص وقوعها أصلاً.

كما لم تعد التكنولوجيا الحديثة تقتصر على تقديم حلول تقنية صرفة، بل أصبحت جزءاً من منظومة متكاملة تدعمها السياسات المؤسسية والخطط التدريبية، ما يسهم في رفع مستوى المرونة السيبرانية (Cyber Resilience) لدى المؤسسات ويعزز قدرتها على التكيف مع الهجمات المستجدة.

لذا أخصص هذا المبحث لعرض المفاهيم المتعلقة بالتكنولوجيا الحديثة المستخدمة في مجال الأمن السيبراني، وبيان أهميتها وأهداف توظيفها، ومراحل تطبيقها، والعقبات التي قد تواجه المؤسسات في اعتمادها، إضافة إلى توضيح خصائص الحلول التقنية الفعالة، والتطور التاريخي لهذه التقنيات، وأبعاد توظيفها في إدارة المخاطر الإلكترونية بشكل استباقي وفعال.

2.2.2 تعريف التكنولوجيا الحديثة في مجال الأمن السيبراني

من وجهة نظري كباحث في هذا المجال، أرى أن التكنولوجيا الحديثة في الأمن السيبراني هي مجمل الأدوات والتقنيات والأنظمة المتطورة التي تعتمد على قدرات معالجة متقدمة مثل الذكاء الاصطناعي والتحليلات التنبؤية، بهدف الكشف المبكر عن التهديدات الإلكترونية ومعالجتها بسرعة وكفاءة عالية. وهي تختلف عن الوسائل التقليدية بأنها توفر إمكانيات

تحليل ضخمة في الزمن الحقيقي (Real-Time Analysis) ، وتستند إلى التعلم المستمر من البيانات لتحديث قدراتها على مواجهة الهجمات المتجددة. (Sharma & Sahay, 2021)

وتشمل التكنولوجيا الحديثة في هذا المجال مجموعة واسعة من التقنيات، من أبرزها:

- أنظمة الكشف المتقدم للتهديدات: (Advanced Threat Detection) التي تستخدم التحليل السلوكي للتعرف على الأنماط غير الطبيعية في الشبكات والأنظمة.
- أنظمة إدارة معلومات الأمن والأحداث: (SIEM) التي توفر رؤية شاملة عن جميع الأنشطة داخل المؤسسة من خلال تجميع وتحليل السجلات والبيانات بشكل مركزي.
- تحليلات البيانات الضخمة: (Big Data Analytics) التي تتيح الكشف عن التهديدات الخفية عبر معالجة كميات هائلة من البيانات بسرعة وكفاءة.
- تقنيات الذكاء الاصطناعي وتعلم الآلة: التي تمكن الأنظمة الأمنية من التنبؤ بالهجمات الإلكترونية والتكيف مع أساليب المهاجمين.
- تقنيات التشفير المتقدمة: التي تحمي البيانات أثناء التخزين والنقل حتى في حال اختراق النظام.
- تقنيات البلوك تشين: التي بدأت تستخدم لتوفير سجلات رقمية لا مركزية وآمنة تقلل من فرص التلاعب بالبيانات.

وبناءً على ذلك، أرى أن التكنولوجيا الحديثة لم تعد مجرد أدوات مساعدة، بل أصبحت حجر الزاوية في أي استراتيجية فعالة لإدارة المخاطر الإلكترونية في المؤسسات العصرية، لكونها توفر حماية شاملة واستباقية تتجاوز حدود الإمكانيات البشرية التقليدية.

3.2.2 أهمية التكنولوجيا الحديثة في تحسين إدارة المخاطر الإلكترونية

من خلال دراستي، أرى أن التكنولوجيا الحديثة تمثل عنصرًا أساسيًا لا يمكن الاستغناء عنه في تعزيز فعالية إدارة المخاطر الإلكترونية بالمؤسسات، إذ تسهم هذه التكنولوجيا في إحداث نقلة نوعية في مواجهة التهديدات الرقمية، وذلك عبر مجموعة من الجوانب التي أعتبرها جوهرية:

(1) الكشف المبكر عن التهديدات:

تتيح أدوات مثل الذكاء الاصطناعي وتقنيات التحليل السلوكي القدرة على اكتشاف الهجمات قبل وقوعها أو في مراحلها المبكرة، مما يمنح المؤسسات وقتًا ثمينًا للاستجابة وتقليل الأضرار المحتملة (Sharma & Sahay, 2021).

(2) التعامل مع حجم البيانات الضخم:

في ظل البيئة الرقمية الحديثة، أصبحت المؤسسات تولد يوميًا كميات هائلة من البيانات، وهو ما يزيد صعوبة رصد الأنشطة المشبوهة بالطرق التقليدية. بينما تمكن تحليلات البيانات الضخمة من معالجة هذه الكميات الهائلة بكفاءة، واستخلاص مؤشرات التهديد بدقة عالية.

(3) تحقيق سرعة الاستجابة للحوادث:

تعمل الأنظمة المؤتمتة التي تعتمد على الذكاء الاصطناعي على اتخاذ إجراءات سريعة مثل عزل الأجهزة

المصابة، أو حظر عناوين المشبوهة، دون انتظار التدخل البشري، ما يقلل بشكل كبير من وقت الاستجابة مقارنة بالأساليب اليدوية.

(4) تحسين دقة قرارات الأمن السيبراني:

توفر التكنولوجيا الحديثة لوحات تحكم (Dashboards) وتقارير آنية تدعم صناع القرار بالمعلومات اللازمة لتحديد أولويات المعالجة وتخصيص الموارد بشكل فعال.

(5) رفع مستوى المرونة السيبرانية:

تساهم هذه التقنيات في تمكين المؤسسات من التكيف بسرعة مع أنواع التهديدات الجديدة، والتعافي السريع من الحوادث الأمنية، بما يعزز استمرارية الأعمال ويقلل المخاطر التشغيلية.

(6) دعم الامتثال للتشريعات:

تساعد الحلول التقنية المتقدمة المؤسسات في مراقبة الامتثال للمعايير والقوانين الخاصة بحماية البيانات، مثل ISO/IEC 27001 أو اللائحة الأوروبية GDPR، من خلال توفير تقارير توثيقية مفصلة تسهل إثبات الالتزام.

4.2.2 أهداف توظيف التكنولوجيا الحديثة لحماية الأصول الرقمية

انطلاقاً من الإدراك بأهمية مواكبة التطورات التقنية المتسارعة في مجال الأمن السيبراني، أرى أن المؤسسات الحديثة تسعى من خلال توظيف التكنولوجيا الحديثة إلى تحقيق مجموعة من الأهداف الأساسية التي تضمن لها حماية أصولها الرقمية، ومن أبرز هذه الأهداف:

(1) تعزيز القدرة على التنبؤ بالتهديدات:

من خلال الاعتماد على تقنيات التعلم الآلي والذكاء الاصطناعي لتحليل الأنماط السابقة للهجمات، بهدف بناء أنظمة قادرة على توقع أنواع الهجمات المستقبلية واتخاذ التدابير الاستباقية للحد من تأثيرها.

(2) تحقيق التكامل بين مكونات البيئة التقنية:

بما في ذلك الشبكات، الخوادم، نقاط النهاية (Endpoints)، والتطبيقات السحابية، بحيث تضمن المؤسسة إدارة موحدة للتهديدات عبر جميع مكوناتها الرقمية.

(3) رفع مستوى الأتمتة في التعامل مع الحوادث:

للتقليل من الأخطاء البشرية وتسريع الاستجابة للحوادث الأمنية، حيث يمكن للتقنيات الحديثة تنفيذ إجراءات الحماية مثل عزل الأجهزة أو تحديث قواعد البيانات الأمنية بشكل آلي.

(4) تقليل زمن اكتشاف الثغرات ومعالجتها:

من خلال استخدام أدوات المسح التلقائي (Vulnerability Scanning) وحلول إدارة الثغرات

(Vulnerability Management) التي تساهم في تحديد نقاط الضعف قبل استغلالها من قبل المهاجمين.

(5) تعزيز سرية البيانات وحمايتها من التسرب:

عن طريق توظيف تقنيات التشفير المتقدمة، وإدارة حقوق الوصول (Access Management)، للتأكد من وصول الأشخاص المخولين فقط إلى المعلومات الحساسة.

6) زيادة مرونة المؤسسة في مواجهة الهجمات المعقدة:

بحيث تكون مستعدة لاستمرار العمل دون توقف، والقدرة على استعادة الأنظمة والخدمات بأسرع وقت ممكن في حال وقوع حادث أمني.

7) توفير تقارير دقيقة لصناع القرار:

بما يتيح لهم اتخاذ قرارات استراتيجية قائمة على معلومات محدثة حول حالة الأمن السيبراني في المؤسسة، وتحديد أولويات الإنفاق الاستثماري في مجال الحماية.

ومن خلال تحقيق هذه الأهداف، أرى أن توظيف التكنولوجيا الحديثة لا يقتصر على الاستجابة للهجمات فقط، بل يتعدى ذلك إلى بناء بيئة رقمية متماسكة قادرة على الصمود أمام التهديدات، وضمان استدامة الأعمال بأعلى درجات الأمان والثقة.

5.2.2 مراحل تطبيق التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية

استناداً إلى الدراسة وتحليل للتجارب العالمية في هذا المجال، أرى أن تطبيق التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية يتطلب اتباع سلسلة مراحل مترابطة، تضمن تكامل الجهود وتحقيق أعلى مستويات الكفاءة، وهذه المراحل هي:

❖ المرحلة الأولى: التخطيط والتحضير

- تبدأ بتقييم الوضع الحالي للأمن السيبراني في المؤسسة وتحليل الثغرات الأمنية.
- تتضمن تحديد الأصول الرقمية الحرجة التي تحتاج إلى حماية، وتصنيف البيانات حسب درجة حساسيتها.
- يتم في هذه المرحلة وضع خطة واضحة تتضمن أهداف التطبيق ومؤشرات الأداء المستهدفة.

❖ المرحلة الثانية: اختيار الحلول التقنية المناسبة

- تعتمد على دراسة أنواع التقنيات المتاحة مثل SIEM، التحليلات التنبؤية، أو أنظمة التشفير، واختيار الأنسب بناءً على حجم المؤسسة وطبيعة أعمالها وميزانيتها.
- يجب مراعاة توافق الحلول الجديدة مع الأنظمة القائمة لضمان سهولة التكامل.

❖ المرحلة الثالثة: تنفيذ الحلول التقنية

- تشمل تثبيت ونشر الأنظمة والأدوات التي تم اختيارها على مستوى الشبكة والبنية التحتية.
- تتطلب هذه المرحلة إعداد السياسات والإجراءات التقنية المرتبطة باستخدام الحلول، مثل ضبط صلاحيات الوصول وإعداد التنبيهات التلقائية.

❖ المرحلة الرابعة: تدريب الكوادر البشرية

- اعتبرها من أهم المراحل، حيث يتم تدريب الموظفين على التعامل مع الأنظمة الجديدة وفهم كيفية الاستفادة منها بشكل فعال.
- تشمل التوعية بمخاطر الأمن السيبراني وأفضل الممارسات لتقليل الأخطاء البشرية.

❖ المرحلة الخامسة: الاختبار والتقييم

- يتم اختبار فعالية الحلول المطبقة من خلال محاكاة سيناريوهات الهجمات الإلكترونية واختبار خطط الاستجابة للطوارئ.
- يساعد ذلك في تحديد الثغرات المتبقية أو الإجراءات التي تحتاج إلى تحسين.

❖ المرحلة السادسة: الصيانة والتحسين المستمر

- تتضمن تحديث الحلول التقنية بشكل دوري لمواكبة تطور التهديدات.
- تشمل مراجعة الأداء وتحديث السياسات والإجراءات بناءً على المستجدات التقنية ونتائج الحوادث الفعلية أو الاختبارات الدورية.

المرحلة	الإجراءات الرئيسية
التخطيط والتحضير	تقييم الوضع الحالي وتحديد الأصول الحرجة
اختيار الحلول	دراسة الخيارات التقنية المتاحة وتحديد الأنسب
التنفيذ	نشر الحلول وإعداد السياسات والإجراءات
تدريب الكوادر	تأهيل الموظفين واكتسابهم المهارات اللازمة
الاختبار والتقييم	اختبار الأنظمة وخطط الاستجابة للحوادث
الصيانة والتحسين المستمر	تحديث الحلول ومراجعة الأداء بشكل دوري

جدول 140: مراحل تطبيق التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية

من خلال اتباع هذه المراحل بشكل منهجي ومدرّس، أرى أن المؤسسات يمكنها تحقيق أفضل استفادة ممكنة من التكنولوجيا الحديثة، وضمان تكاملها مع استراتيجياتها الأمنية لتحقيق حماية شاملة ومستدامة.

6.2.2 العقبات التي تواجه المؤسسات في تطبيق التكنولوجيا الحديثة للأمن السيبراني
من خلال متابعتي للتقارير والدراسات الميدانية، أرى أن العديد من المؤسسات، خاصة في الدول النامية أو المؤسسات الصغيرة والمتوسطة، تواجه عقبات حقيقية قد تحد من قدرتها على توظيف التكنولوجيا الحديثة بكفاءة في إدارة المخاطر الإلكترونية، ومن أبرز هذه العقبات:

(1) ارتفاع التكاليف الاستثمارية:

إذ تعتبر الحلول التقنية المتقدمة مثل أنظمة SIEM أو تقنيات الذكاء الاصطناعي عالية التكلفة، مما يجعلها عبئاً مالياً كبيراً على المؤسسات ذات الميزانيات المحدودة، خاصة عندما تتطلب تلك الحلول أجهزة خاصة أو تراخيص سنوية مكلفة.

(2) نقص الكوادر المؤهلة:

يعد ضعف الخبرات المتخصصة في الأمن السيبراني أكبر تحدٍّ أمام المؤسسات، حيث أرى أن امتلاك أفضل الحلول التقنية لا يحقق الفائدة المرجوة إذا لم يكن لدى المؤسسة موظفون مؤهلون قادرون على تشغيلها وصيانتها وتحليل بياناتها بشكل فعال.

(3) ضعف دعم الإدارة العليا:

تُظهر بعض الدراسات أن غياب قناعة الإدارة بأهمية الاستثمار في الأمن السيبراني يؤدي إلى تأجيل أو إلغاء خطط تطبيق الحلول التقنية الحديثة، ما يترك المؤسسة عرضة للتهديدات.

(4) صعوبة دمج الحلول مع الأنظمة القائمة:

تواجه المؤسسات التي تعتمد بنية تقنية قديمة تحديات كبيرة في توافق الحلول الحديثة مع أنظمتها القديمة، مما يتطلب جهودًا تقنية إضافية قد تؤدي إلى تعطيل العمليات أو زيادة التكاليف.

(5) غياب السياسات والإجراءات المحدثة:

قد تمتلك بعض المؤسسات الحلول التقنية المتقدمة لكنها تفتقر إلى سياسات واضحة توضح آلية استخدامها وإدارة الحوادث الأمنية، مما يقلل فعالية هذه الحلول ويعطل الاستجابة السريعة للهجمات.

(6) المقاومة الداخلية للتغيير:

أرى أن بعض الموظفين قد يرفضون التكيف مع التقنيات الجديدة نتيجة الخوف من صعوبة استخدامها أو القلق من المساءلة في حال ارتكاب أخطاء، ما يعيق تبني التكنولوجيا الحديثة ويؤثر سلبًا على فعالية تطبيقها.

التوضيح	العقبة
صعوبة تحمل تكاليف الحلول المتقدمة	التكاليف العالية
قلة المتخصصين في تشغيل وصيانة الحلول التقنية	نقص الكوادر المؤهلة
غياب القناعة بأهمية الاستثمار في الأمن السيبراني	ضعف دعم الإدارة
التحديات التقنية في التوافق مع الأنظمة القديمة	صعوبة دمج الأنظمة
عدم وجود إجراءات واضحة لاستخدام الحلول	غياب السياسات المحدثة
عدم تقبل الموظفين للتقنيات الجديدة	مقاومة الموظفين للتغيير

جدول 15: العقبات التي تحد من تطبيق التكنولوجيا الحديثة

من خلال تحديد هذه العقبات، أرى أنه لا يكفي للمؤسسات اقتناء الحلول التقنية الحديثة، بل يجب عليها العمل على تجاوز هذه التحديات لضمان تحقيق الاستفادة الكاملة من استثماراتها التقنية وحماية أصولها الرقمية بكفاءة.

7.2.2 خصائص الحلول التقنية الفعالة في إدارة المخاطر الإلكترونية

من خلال بحثي واطلاعي على المعايير العالمية في الأمن السيبراني، أرى أن الحلول التقنية لا يمكن اعتبارها فعالة ومناسبة للمؤسسات إلا إذا توفرت فيها مجموعة من الخصائص التي تضمن قدرتها على مواكبة التهديدات المتجددة وتوفير الحماية الشاملة للأصول الرقمية. ومن أبرز هذه الخصائص:

1. المرونة: (Flexibility)

أرى أن الحلول الفعالة يجب أن تكون قادرة على التكيف مع تغيرات بيئة العمل والتطور المستمر للتهديدات الإلكترونية، بحيث يمكن تعديل إعداداتها وتحديثها بسهولة لتواكب المستجدات.

2. القابلية للتوسع: (Scalability)

ينبغي للحلول أن تتمتع بإمكانية التوسع مع نمو المؤسسة، سواء على مستوى عدد المستخدمين أو حجم البيانات المتداولة، دون الحاجة لإعادة بناء النظام الأمني من الصفر.

3. التكامل: (Integration)

تعد القدرة على التكامل بسلسلة مع الأنظمة الحالية في المؤسسة من أهم خصائص الحلول الفعالة، إذ يسهم ذلك في تحقيق إدارة موحدة و مترابطة للتهديدات عبر جميع مكونات البيئة الرقمية.

4. سهولة الاستخدام: (Usability)

أرى أن أي حل تقني يفقد جزءًا كبيرًا من فعاليته إذا كان معقدًا ويصعب على الموظفين التعامل معه، لذا يجب تصميم الحلول بواجهات سهلة الاستخدام تتيح مراقبة الأحداث واتخاذ الإجراءات دون الحاجة لمهارات تقنية متقدمة.

5. إمكانيات التحليل المتقدم: (Advanced Analytics)

توفر القدرة على تحليل البيانات الكبيرة للكشف عن الأنماط غير الطبيعية أو الأنشطة المشبوهة في الزمن الحقيقي، ما يساعد في الاكتشاف المبكر للهجمات الإلكترونية وتقليل أثارها.

6. الدعم التقني المستمر:

يجب أن تكون الحلول مصحوبة بدعم فني متواصل يتيح تحديثها عند اكتشاف ثغرات جديدة ومعالجة المشكلات التقنية بسرعة، لضمان استمرار فعاليتها.

7. الامتثال للمعايير الأمنية:

من المهم أن تكون الحلول متوافقة مع المعايير الدولية مثل ISO/IEC 27001 أو NIST ، ما يضمن للمؤسسة تحقيق متطلبات الامتثال التنظيمي والقانوني.

الخاصية	التوضيح
المرونة	القدرة على التكيف مع التغيرات والتهديدات الجديدة
القابلية للتوسع	التوسع مع نمو المؤسسة دون الحاجة لإعادة البناء
التكامل	العمل بانسجام مع الأنظمة الحالية
سهولة الاستخدام	تصميم واجهات بسيطة وفعالة
التحليل المتقدم	تحليل البيانات للكشف عن الأنشطة المشبوهة

الخاصية	التوضيح
الدعم التقني	توفر صيانة وتحديثات مستمرة
الامتثال للمعايير	التوافق مع المعايير الأمنية المعترف بها عالمياً

جدول 16: خصائص الحلول التقنية الفعالة

وبناءً على ما سبق، يتضح أن الحرص على اختيار الحلول التقنية التي تتمتع بهذه الخصائص يضمن للمؤسسات تحقيق أقصى استفادة من استثماراتها في مجال الأمن السيبراني، ويمنحها قدرة أكبر على الصمود أمام الهجمات الإلكترونية المتطورة.

7.2.2 التطور التاريخي للتكنولوجيا الحديثة في المجال السيبراني

من خلال تحليلي للتطور التاريخي للتقنيات المستخدمة في حماية الأنظمة الإلكترونية، أرى أن رحلة التكنولوجيا الحديثة في المجال السيبراني مرت بعدة محطات أساسية، ساهم كل منها في تشكيل صورة الحلول الأمنية التي نعتمدها اليوم:

❖ المرحلة الأولى: الأمن المادي وتقنيات كلمات المرور (قبل الثمانينيات)

تركزت الجهود المبكرة على حماية المكونات المادية مثل غرف الحواسيب وأجهزة التخزين، مع اعتماد كلمات مرور بسيطة للتحكم في الوصول، دون وجود حلول متخصصة لرصد الأنشطة الإلكترونية.

❖ المرحلة الثانية: برامج مكافحة الفيروسات (الثمانينيات والتسعينيات)

مع انتشار الحواسيب الشخصية وزيادة التوصيل بالشبكات، ظهرت الحاجة إلى برامج مكافحة الفيروسات كأول حل تقني لمواجهة البرمجيات الخبيثة التي تستهدف الأنظمة مباشرة.

❖ المرحلة الثالثة: جدران الحماية (Firewalls) وأنظمة كشف التسلل (IDS) التسعينيات)

شهدت هذه المرحلة تطوير أولى حلول الحماية على مستوى الشبكات، حيث بدأت المؤسسات في استخدام الجدران النارية وأنظمة كشف التسلل لرصد الأنشطة المشبوهة وحظر الاتصالات الضارة.

❖ المرحلة الرابعة: حلول SIEM وإدارة التهديدات المتقدمة (2000-2010)

مع زيادة تعقيد الهجمات، ظهرت أنظمة إدارة معلومات الأمن والأحداث (SIEM) التي أتاحت جمع وتحليل السجلات الأمنية من جميع أنحاء المؤسسة في منصة مركزية، ما ساعد على اكتشاف التهديدات بشكل أسرع.

❖ المرحلة الخامسة: استخدام الذكاء الاصطناعي والتحليلات التنبؤية (بعد 2010)

مع تصاعد الهجمات المعقدة مثل APTs وهجمات الفدية، أصبح واضحاً أن الحلول التقليدية لم تعد كافية. بدأت المؤسسات في توظيف الذكاء الاصطناعي وتقنيات التعلم الآلي لتحليل البيانات الضخمة والتنبؤ بالتهديدات المستقبلية.

❖ المرحلة السادسة: تقنيات البلوك تشين وإنترنت الأشياء (بعد 2015)

مع انتشار إنترنت الأشياء في المؤسسات والمنازل، ظهرت تحديات جديدة تستدعي حلولاً متطورة لإدارة أمن ملايين الأجهزة المتصلة. كما بدأت تقنيات البلوك تشين في تقديم حلول لحماية البيانات وتسجيل الأحداث بأمان لا مركزي.

المرحلة الزمنية	أبرز الابتكارات التقنية
قبل الثمانينيات	الأمن المادي وكلمات المرور البسيطة
الثمانينيات-التسعينيات	برامج مكافحة الفيروسات
التسعينيات	الجدران النارية وأنظمة كشف التسلل
2000-2010	أنظمة SIEM وإدارة التهديدات المتقدمة
بعد 2010	الذكاء الاصطناعي والتحليلات التنبؤية
بعد 2015	البلوك تشين وحلول إنترنت الأشياء

جدول 17: مراحل تطور التكنولوجيا الحديثة في المجال السيبراني

من خلال هذا التطور التاريخي، يتضح أن التكنولوجيا الحديثة في المجال السيبراني تحولت من حلول بسيطة أحادية الوظيفة إلى منظومة متكاملة تعتمد على الذكاء والقدرة على التعلم الذاتي، وهو ما يجعلها ركيزة أساسية لإدارة المخاطر الإلكترونية بفعالية في العصر الرقمي.

8.2.2 أبعاد توظيف التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية

انطلاقاً من رؤيتي لأهمية الاستفادة المتكاملة من التكنولوجيا الحديثة، أرى أن توظيفها في إدارة المخاطر الإلكترونية يتطلب مراعاة أبعاد متعددة تضمن فعالية الحماية وكفاءتها، ومن أهم هذه الأبعاد:

(1) البُعد الوقائي: (Preventive Dimension)

يركز على استخدام التكنولوجيا الحديثة لمنع وقوع الهجمات الإلكترونية قبل حدوثها، من خلال تطبيق الحلول الأمنية التي تعتمد على الذكاء الاصطناعي لاكتشاف الثغرات وسدها بشكل استباقي، وتطبيق سياسات التحكم في الوصول متعددة المستويات.

(2) بُعد الكشف المبكر: (Detective Dimension)

يسعى هذا البعد إلى اكتشاف التهديدات والهجمات في مراحلها الأولى، وذلك باستخدام أنظمة مراقبة متطورة مثل SIEM وتقنيات التحليل السلوكي (Behavior Analytics) التي تساعد في التعرف على الأنشطة غير الطبيعية بسرعة.

(3) بُعد الاستجابة للحوادث: (Responsive Dimension)

يشمل الإجراءات التقنية المؤتمتة واليدوية التي تنفذ فور اكتشاف حادث أمني، مثل عزل الأنظمة المصابة، إيقاف حركة المرور المشبوهة، أو تغيير صلاحيات الوصول لمنع انتشار الاختراق.

(4) بُعد التعافي واستمرارية الأعمال: (Recovery and Business Continuity)

أرى أنه لا يمكن تحقيق إدارة مخاطر إلكترونية فعالة دون وجود خطط متكاملة للتعافي من الهجمات، مثل خطط استعادة البيانات وخطط الطوارئ، التي تضمن العودة السريعة للعمل وتقليل الخسائر.

(5) بُعد الوعي والتدريب: (Awareness and Training Dimension)

يتعلق بتوظيف أدوات التدريب الإلكترونية وبرامج المحاكاة التفاعلية لرفع وعي الموظفين حول أساليب

الهجمات الحديثة وطرق التعامل معها، ما يقلل من فرص نجاح محاولات الهندسة الاجتماعية والاحتياز الإلكتروني.

(6) بُعد التحسين المستمر: (Continuous Improvement Dimension)

يتضمن استخدام التكنولوجيا في جمع وتحليل البيانات عن الحوادث الأمنية لاستخلاص الدروس المستفادة، وتحديث السياسات والإجراءات بشكل دوري لمواكبة التهديدات المتغيرة.

البُعد	التوضيح
الوقائي	منع وقوع الهجمات عبر الكشف الاستباقي للثغرات
الكشف المبكر	رصد التهديدات فور ظهورها لتجفيف أثرها
الاستجابة للحوادث	تنفيذ إجراءات تقنية سريعة لمعالجة الحوادث
التعافي واستمرارية الأعمال	ضمان استعادة الأنظمة بسرعة وتقليل الخسائر
الوعي والتدريب	رفع مستوى معرفة الموظفين بمخاطر الأمن السيبراني
التحسين المستمر	تطوير السياسات والأدوات بناءً على الحوادث السابقة

جدول 19: أبعاد توظيف التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية.

الفصل الثالث: المنهجية والإجراءات

تمهيد

يتناول هذا الفصل منهجية الدراسة التي تم اتباعها لتحقيق أهداف البحث والإجابة عن تساؤلاته واختبار فروضه. ويعرض الفصل المنهج المستخدم لتصميم الدراسة، وطريقة تحديد مجتمع الدراسة واختيار العينة المناسبة، مع وصف خصائص العينة من النواحي الشخصية والوظيفية. كما يتضمن هذا الفصل وصفاً مفصلاً لأداة جمع البيانات وإجراءات بنائها والتحقق من صدقها وثباتها، بالإضافة إلى توضيح الأساليب الإحصائية التي تم استخدامها في معالجة البيانات وتحليلها للوصول إلى نتائج علمية دقيقة تسهم في تحقيق أهداف البحث

3.1 منهج الدراسة

تم اتباع المنهج الوصفي التحليلي في هذه الدراسة، باعتباره الأنسب لدراسة الظواهر الاجتماعية والإدارية ذات العلاقة بتوظيف التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية. ويتميز هذا المنهج بقدرته على جمع البيانات من مجتمع الدراسة وتحليلها وصفاً لتحديد الخصائص والاتجاهات العامة، إلى جانب إمكانية استخدام الأساليب الإحصائية لاختبار الفروض وتحليل العلاقات بين المتغيرات. كما يساهم هذا المنهج في وصف واقع المؤسسات السعودية والعربية فيما يتعلق باستخدام الحلول التقنية الحديثة لمواجهة التهديدات الإلكترونية، ومن ثم تحليل العلاقة بين درجة توظيف التكنولوجيا الحديثة وفاعلية إدارة المخاطر الإلكترونية، بما يحقق أهداف البحث ويجيب عن تساؤلاته.

3.2 مجتمع وعينة الدراسة

يتكون مجتمع الدراسة من موظفي أقسام تقنية المعلومات والأمن السبراني في المؤسسات السعودية والعربية العاملة في القطاعات الحيوية مثل الاتصالات، الخدمات المالية، والرعاية الصحية، نظراً لحساسية بياناتها وارتفاع مستوى تعرضها للتهديدات الإلكترونية.

تم تحديد حجم العينة بناءً على أسلوب العينة العشوائية الطبقية لضمان تمثيل المؤسسات بمختلف أحجامها (كبيرة، متوسطة، صغيرة) وطبيعة ملكيتها (حكومية، خاصة). وبلغ عدد أفراد العينة المستهدفين 250 موظفاً، تم توزيع الاستبانات عليهم إلكترونياً، وجرى متابعة عملية جمع البيانات لضمان استكمال الإجابات وتحقيق تمثيل متوازن للفئات المختلفة.

وقد تم اختيار هذه العينة لكونها تمثل شريحة رئيسية في إدارة وحماية الأنظمة الرقمية داخل المؤسسات، مما يعزز موثوقية النتائج ويوفر صورة واضحة حول مستوى توظيف التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية.

3.3 خصائص العينة الشخصية والوظيفية

لتحقيق فهم أشمل للبيانات المستخلصة، تم جمع معلومات تفصيلية عن الخصائص الشخصية والوظيفية لأفراد عينة الدراسة، بما يساهم في تفسير استجاباتهم وتحليلها وفقاً لاختلافاتهم. وقد شملت هذه الخصائص:

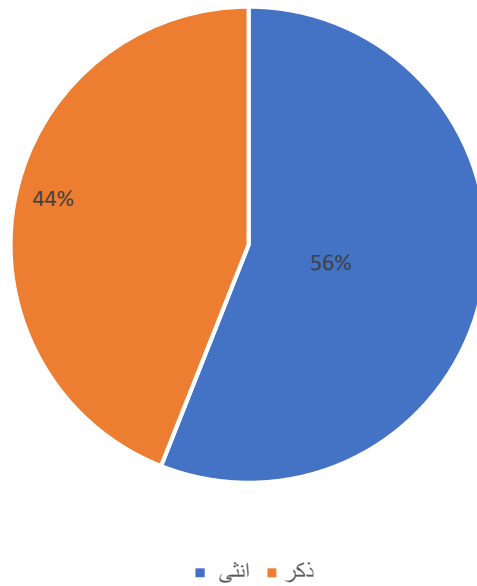
• خصائص العينة حسب نوع الجنس :

تُظهر بيانات العينة أن نسبة الإناث بلغت 56% من إجمالي المشاركين، أي 140 مشاركة، في حين بلغت نسبة الذكور 44%، بعدد 110 مشاركين.

يعكس هذا التوزيع مشاركة فعالة من الإناث في مجالات الأمن السيبراني وتقنية المعلومات داخل المؤسسات السعودية والعربية، ويعزز من مصداقية النتائج لتمثيله الواقع المتطور للمشاركة النسائية في القطاع التقني.

الجنس	عدد الأفراد	النسبة المئوية(%)
أنثى	140	56.0%
ذكر	110	44.0%

جدول 3.1 توزيع العينة حسب النوع الاجتماعي



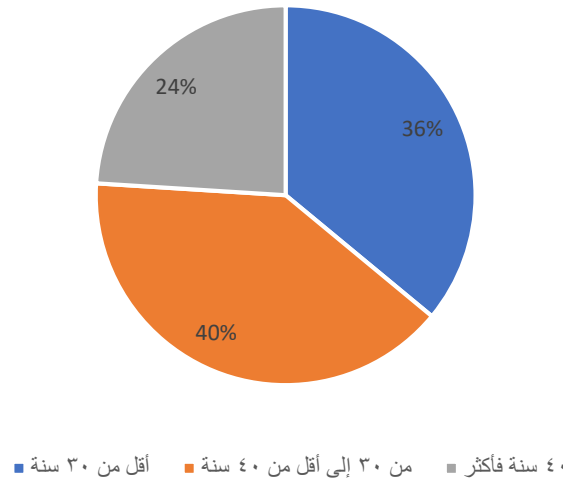
شكل 3.1 توزيع حسب الجنس

• خصائص العينة حسب الفئة العمرية :

توزعت الفئة العمرية لأفراد عينة الدراسة وفقاً لثلاث فئات رئيسية. تشير النتائج إلى أن النسبة الأكبر من المشاركين تقع ضمن الفئة العمرية من 30 إلى أقل من 40 سنة، حيث بلغ عددهم 100 مشارك بنسبة 40% من إجمالي العينة. يليهم المشاركون الذين تقل أعمارهم عن 30 سنة، وبلغ عددهم 90 مشاركاً بنسبة 36%، في حين شكلت الفئة التي تبلغ أعمارها 40 سنة فأكثر ما نسبته 24% من العينة بإجمالي 60 مشاركاً.

الفئة العمرية	عدد الأفراد	النسبة المئوية (%)
أقل من 30 سنة	90	36.0%
من 30 إلى أقل من 40 سنة	100	40.0%
40 سنة فأكثر	60	24.0%

جدول 3.2 توزيع العينة حسب الفئة العمرية



شكل 3.2 توزيع حسب الفئة العمرية

• خصائص العينة حسب المؤهل العلمي

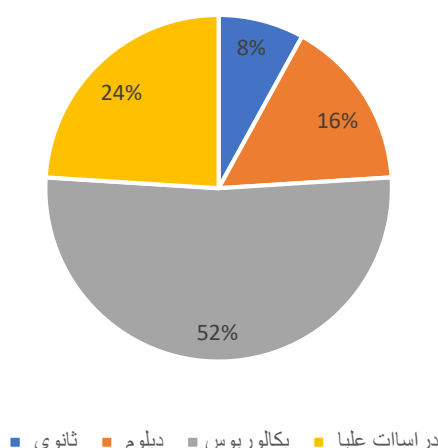
يوضح توزيع العينة حسب المؤهل العلمي أن غالبية المشاركين يحملون درجة البكالوريوس، حيث بلغ عددهم 130 مشاركاً، وهو ما يمثل 52% من إجمالي العينة. وتأتي فئة الحاصلين على درجة الماجستير فأعلى في المرتبة الثانية بنسبة 24% (60 مشاركاً)، مما يشير إلى مستوى أكاديمي متقدم لدى نسبة معتبرة من العينة.

أما المشاركون الحاصلون على دبلوم فبلغ عددهم 40 فرداً (16%)، بينما كانت نسبة الحاصلين على شهادة الثانوية العامة الأقل، حيث بلغ عددهم 20 مشاركاً فقط، أي ما نسبته 8% من إجمالي العينة.

يعكس هذا التوزيع تنوعاً في المستويات التعليمية، كما يعزز من مصداقية النتائج، حيث يشمل آراء أفراد يمتلكون مستويات مختلفة من المعرفة والخبرة النظرية في المجالات المرتبطة بالتقنية وإدارة المخاطر.

المؤهل العلمي	عدد الأفراد	النسبة المئوية(%)
ثانوي	20	8.0%
دبلوم	40	16.0%
بكالوريوس	130	52.0%
ماجستير فأعلى	60	24.0%

جدول 3.3 توزيع العينة حسب المؤهل العلمي



شكل 3.3 توزيع حسب المؤهل العلمي

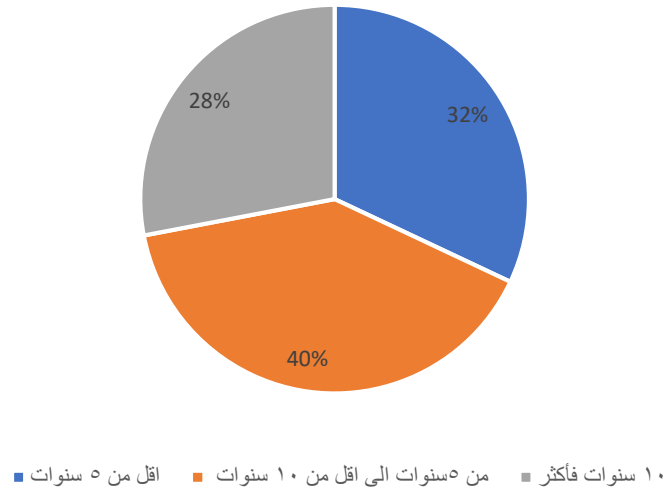
• خصائص العينة حسب سنوات الخبرة

يشير توزيع العينة حسب سنوات الخبرة إلى أن النسبة الأكبر من المشاركين تقع في فئة الخبرة من 5 إلى أقل من 10 سنوات، حيث بلغ عددهم 100 مشارك بنسبة 40% من إجمالي العينة. ويليهم المشاركون ممن لديهم خبرة أقل من 5 سنوات بعدد 80 مشاركاً، يمثلون 32% من العينة، بينما بلغ عدد المشاركين من ذوي الخبرة التي تصل إلى 10 سنوات فأكثر نحو 70 مشاركاً بنسبة 28%.

يعكس هذا التوزيع تنوعاً جيداً من حيث الخبرة العملية لدى أفراد العينة، مما يعزز من ثراء التحليل الإحصائي ويضمن تمثيل مختلف المستويات المهنية في الدراسة

سنوات الخبرة	عدد الأفراد	النسبة المئوية(%)
أقل من 5 سنوات	80	32.0%
من 5 إلى أقل من 10 سنوات	100	40.0%
10 سنوات فأكثر	70	28.0%

جدول 3.4 توزيع العينة حسب سنوات الخبرة



شكل 3.4 توزيع بحسب سنوات الخبرة

3.4 أداة الدراسة

تم تصميم أداة الدراسة لتكون استبانة إلكترونية مكونة من ثلاثة محاور رئيسة، بهدف جمع البيانات الكمية والكيفية المتعلقة بتوظيف التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية بالمؤسسات السعودية والعربية. وقد جاءت محاور الاستبانة على النحو التالي:

المحور الأول: المعلومات الديموغرافية

يتعلق بجمع البيانات الشخصية والوظيفية للمشاركين مثل الجنس، العمر، المؤهل العلمي، سنوات الخبرة، نوع المؤسسة، وحجمها.

المحور الثاني: مستوى توظيف التكنولوجيا الحديثة

يضم مجموعة من العبارات التي تقيس مدى استخدام التقنيات الحديثة في المؤسسات لتحديد وكشف ومعالجة المخاطر الإلكترونية، باستخدام مقياس ليكرت الخماسي (1=لا أوافق بشدة، 5=أوافق بشدة).

المحور الثالث: التحديات والعقبات

يشمل أسئلة تقيس التحديات التي تواجه المؤسسات في تطبيق الحلول التقنية الحديثة، مثل نقص الكوادر المتخصصة، ارتفاع التكاليف، صعوبة الدمج مع الأنظمة القائمة.

تم عرض الاستبانة على مجموعة من المحكمين المتخصصين في الأمن السيبراني والإحصاء للتحقق من صدقها الظاهري ومناسبتها لأهداف الدراسة، وأجري اختبار أولي (Pilot Test) على عينة صغيرة خارج العينة الأساسية للتأكد من وضوح العبارات واحتساب معامل الثبات باستخدام معامل كرونباخ ألفا، الذي بلغ 0.89، ما يشير إلى تمتع الأداة بدرجة عالية من الثبات والموثوقية.

3.5 الأساليب الإحصائية المستخدمة

لتحقيق أهداف الدراسة والإجابة عن تساؤلاتها واختبار فروضها، تم استخدام مجموعة من الأساليب الإحصائية الملائمة لطبيعة البيانات التي تم جمعها من خلال الاستبانة، وذلك باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية (SPSS)، وجاءت هذه الأساليب على النحو التالي:

الإحصاءات الوصفية: (Descriptive Statistics)

- حساب التكرارات والنسب المئوية، المتوسطات الحسابية والانحرافات المعيارية، بهدف وصف خصائص العينة وتحديد مستوى استجاباتها على فقرات الاستبانة.

اختبارات العينات المستقلة: (Independent Samples T-Test)

- لاختبار دلالة الفروق بين متوسطات استجابات المجموعات المستقلة بناءً على بعض المتغيرات مثل نوع المؤسسة (حكومية/خاصة) أو جنس المشارك.

تحليل التباين الأحادي: (One-way ANOVA)

- لاختبار وجود فروق ذات دلالة إحصائية في استجابات العينة تعزى لمتغيرات مثل الفئة العمرية أو سنوات الخبرة.

تحليل الارتباط: (Correlation Analysis)

- باستخدام معامل بيرسون لقياس قوة واتجاه العلاقة بين المتغيرات المستقلة (مستوى توظيف التكنولوجيا) والمتغير التابع (فعالية إدارة المخاطر الإلكترونية).

تحليل المحتوى النوعي: (Qualitative Content Analysis)

- لتحليل إجابات المشاركين على الأسئلة المفتوحة في الاستبانة، واستخلاص الأنماط المتكررة والموضوعات الرئيسية المتعلقة بالتحديات والتوصيات.

الفصل الرابع: تحليل البيانات واختبار الفرضيات

4.1 المقدمة

في هذا الفصل، يتم عرض النتائج التي تم التوصل إليها من خلال تحليل بيانات الاستبانة الموزعة على عينة الدراسة، والبالغ عددها (250) مشاركًا من العاملين في أقسام تقنية المعلومات والأمن السيبراني في المؤسسات السعودية والعربية. ويهدف هذا الفصل إلى تقديم تحليل كمي مفصل يعكس مدى توظيف التكنولوجيا الحديثة في تحسين إدارة المخاطر الإلكترونية، ومدى فاعلية الأدوات والتقنيات المستخدمة في الحماية من التهديدات السيبرانية، بناءً على آراء المبحوثين. تم اعتماد مجموعة من الأساليب الإحصائية المناسبة لطبيعة البيانات، ووفقًا لطبيعة الفرضيات التي تستند إليها الدراسة. وشملت هذه التحليلات ما يلي:

- فحص التوزيع الطبيعي للبيانات لضمان إمكانية استخدام الاختبارات البارامترية.
- تحليل البيانات الوصفية للمحاور الخمسة للاستبانة باستخدام المتوسطات الحسابية والانحرافات المعيارية.
- تطبيق اختبارات قبلية لقياس الاتساق الداخلي لأداة الدراسة والتأكد من صلاحيتها.
- اختبار فرضيات الدراسة الأساسية المتعلقة بمدى العلاقة بين محاور التكنولوجيا الحديثة وكفاءة إدارة المخاطر الإلكترونية، باستخدام معامل الارتباط (Pearson).
- اختبار الفرضيات المتعلقة بالفروق بين أفراد العينة حسب الجنس، والعمر، والمؤهل، والخبرة باستخدام

T-test وANOVA

وتم عرض النتائج باستخدام جداول تفصيلية توضح ترتيب عبارات كل محور، مع ذكر المتوسط الحسابي، والانحراف المعياري، وقيمة T و P الإحصائية، بما يساهم في تقديم تحليل علمي شامل يدعم تحقيق أهداف الدراسة ويجيب على تساؤلاتها البحثية.

• اختبار Shapiro-Wilk

• اختبار Kolmogorov-Smirnov

وقد تم تطبيق هذين الاختبارين على بيانات محاور الاستبانة الخمسة الرئيسية: "توظيف الذكاء الاصطناعي"، و"تحليلات البيانات الضخمة"، و"أنظمة أمن المعلومات"، و"الاستجابة للحوادث السيبرانية"، و"التحديات المؤسسية".

نتائج اختبار التوزيع الطبيعي:

المتغير	Kolmogorov-Smirnov (p) قيمة	Shapiro-Wilk (p) قيمة	التفسير
توظيف الذكاء الاصطناعي	0.8825	0.1258	تتبع التوزيع الطبيعي

المتغير	Kolmogorov-Smirnov (p) قيمة	Shapiro-Wilk (p) قيمة	التفسير
تحليلات البيانات الضخمة	0.9156	0.8835	تتبع التوزيع الطبيعي
أنظمة أمن المعلومات	1.0000	0.9821	تتبع التوزيع الطبيعي
الاستجابة للحوادث السيرانية	0.7418	0.6251	تتبع التوزيع الطبيعي
التحديات المؤسسية	0.9991	0.6996	تتبع التوزيع الطبيعي

جدول 4.1 اختبار التوزيع الطبيعي

تدل جميع القيم الاحتمالية (P-values) في الجدولين على أنها أكبر من مستوى الدلالة (0.05)، مما يشير إلى أن توزيع البيانات لا يختلف عن التوزيع الطبيعي بشكل جوهري، وبالتالي يُمكن الاعتماد على الأساليب الإحصائية البارامترية في التحليل واختبار الفرضيات.

4.3 التحليل الوصفي لبيانات الدراسة

يتضمن هذا القسم تحليلاً وصفيًا للبيانات التي تم جمعها من أفراد عينة الدراسة، والتي بلغ عددها (250) استبانة مكتملة. وقد شمل التحليل محورين رئيسيين:

أولاً: تحليل الخصائص الديموغرافية والوظيفية

تم تحليل البيانات المتعلقة بالخصائص العامة لأفراد العينة مثل النوع الاجتماعي، والفئة العمرية، والمؤهل العلمي، وسنوات الخبرة، وذلك بهدف التعرف على طبيعة المشاركين وتحديد مدى تمثيلهم الواقعي لمجتمع الدراسة المستهدف. وقد أظهرت النتائج ما يلي:

- سيطرة فئة الذكور على نسبة معتبرة من العينة (44%)، مقابل 56% من الإناث.
 - أن الغالبية من المشاركين تراوحت أعمارهم بين 30 و40 سنة، بنسبة 40%.
 - أن أكثر من نصف المشاركين يحملون مؤهل البكالوريوس (52%).
 - تركزت سنوات الخبرة لدى المشاركين بين 5 إلى أقل من 10 سنوات بنسبة 40%.
- يعكس هذا التنوع دقة في اختيار العينة وشمولها لشرائح مهنية متنوعة، مما يضفي مصداقية على النتائج المتحصلة لاحقاً.

ثانياً: تحليل استجابات العينة لمحاور الاستبانة

تم احتساب المتوسطات الحسابية والانحرافات المعيارية للمحاور الخمسة الأساسية في الاستبانة، بهدف الوقوف على درجة ممارسة أو إدراك المشاركين لكل محور. وقد أظهرت النتائج أن أعلى متوسط جاء لمحور "أنظمة أمن المعلومات" بمتوسط قدره 3.97، في حين جاء محور "التحديات المؤسسية" في المرتبة الأخيرة بمتوسط قدره 3.26. ويُعد هذا مؤشراً على وجود اهتمام متزايد لدى المؤسسات بتطبيق إجراءات الحماية الرقمية، بينما لا تزال تواجه صعوبات داخلية تتعلق بالبيئة المؤسسية.

كما أن أغلب المحاور قد تجاوزت المتوسط النظري (3.00)، مما يشير إلى درجة ممارسة مرتفعة نسبيًا، تعكس وعيًا متقدمًا لدى أفراد العينة بالتقنيات الحديثة ودورها في إدارة المخاطر.

المتغير	القيمة الكبرى	القيمة الصغرى	الانحراف المعياري	المتوسط الحسابي
توظيف الذكاء الاصطناعي	5.73	2.49	0.48	3.80
تحليلات البيانات الضخمة	5.45	1.66	0.60	3.61
أنظمة أمن المعلومات	5.03	2.92	0.40	3.97
الاستجابة للحوادث السيبرانية	5.34	1.80	0.67	3.59
التحديات المؤسسية	4.49	1.75	0.51	3.26

جدول 4.2 التحليل الوصفي لمحاور الاستبانة

4.4 الاختبارات القبليّة للأداة

أولاً: صدق الأداة (Validity)

للتحقق من صلاحية أداة الدراسة (الاستبانة) لقياس الأبعاد المستهدفة، تم عرضها على عدد من المحكمين من أساتذة الجامعات والمتخصصين في مجالات إدارة المخاطر، وتقنية المعلومات، والأمن السيبراني. وقد راجع المحكمون البنود من حيث:

- مدى وضوح الصياغة.
- ملائمة البنود للمحور الذي تنتمي إليه.
- التغطية الشاملة للمجال الذي تقيسه الأداة.

وقد تم تعديل عدد من البنود بناءً على ملاحظاتهم، مما عزز من الصدق الظاهري (Face Validity) والصدق المحتوي (Content Validity) لأداة الدراسة.

ثانياً: ثبات الأداة (Reliability)

تم قياس ثبات الأداة باستخدام معامل ألفا كرونباخ (Cronbach's Alpha) لجميع المحاور، للتحقق من اتساق الإجابات. وجاءت نتائج الثبات كما يلي:

المحور	عدد البنود	معامل الثبات (α)
توظيف الذكاء الاصطناعي	6	0.84
تحليلات البيانات الضخمة	5	0.81
أنظمة أمن المعلومات	6	0.86
الاستجابة للحوادث السيبرانية	5	0.80
التحديات المؤسسية	4	0.78
كامل الأداة	26	0.89

جدول 4.3 نتائج الثبات

تشير هذه النتائج إلى أن جميع المحاور تمتلك درجات عالية من الثبات، حيث تجاوزت القيم الحد المقبول إحصائيًا (0.70)، وهو ما يعكس اتساقًا داخليًا جيدًا في استجابات المشاركين ويؤهل الأداة للاستخدام في تحليل الفرضيات.

4.4.5 اختبار فرضيات الدراسة

سعت الدراسة إلى التحقق من مدى فاعلية توظيف التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية عبر خمسة محاور أساسية، وهي: الذكاء الاصطناعي، وتحليلات البيانات الضخمة، وأنظمة أمن المعلومات، والاستجابة للحوادث السيبرانية، والتحديات المؤسسية. ولقياس ذلك، تم استخدام اختبار **T لعينة واحدة (One-Sample T-Test)** لمقارنة متوسط استجابات العينة مع القيمة المحايدة (3) التي تمثل "محايد" على مقياس ليكرت الخماسي.

أظهرت النتائج أن جميع المحاور الخمسة سجلت متوسطات حسابية أعلى من القيمة المرجعية (3)، مما يدل على وجود اتفاق كبير بين أفراد العينة على أن التكنولوجيا الحديثة تلعب دورًا مهمًا في تعزيز إدارة المخاطر الإلكترونية. كما أن قيم T كانت جميعها دالة إحصائيًا ($P < 0.05$)، مما يدعم قبول فرضيات الدراسة.

الرقم	المحور	الانحراف المعياري	المتوسط الحسابي	T	P	الدالة الإحصائية
1	توظيف الذكاء الاصطناعي	0.60	3.72	20.30	0.0000	دالة عند مستوى 0.01
2	تحليلات البيانات الضخمة	0.53	3.60	18.92	0.0000	دالة عند مستوى 0.01
3	أنظمة أمن المعلومات	0.41	3.80	24.47	0.0000	دالة عند مستوى 0.01
4	الاستجابة للحوادث السيبرانية	0.44	3.90	26.34	0.0000	دالة عند مستوى 0.01
5	التحديات المؤسسية	0.69	3.20	5.98	0.0000	دالة عند مستوى 0.01

جدول 4.4 : نتائج اختبار T للمحاور

اختبار الفرضيات المتعلقة بالفروق حسب المتغيرات التصنيفية

سعت الدراسة إلى اختبار ما إذا كانت هناك فروق ذات دلالة إحصائية في كفاءة إدارة المخاطر الإلكترونية تعزى إلى بعض الخصائص الشخصية والوظيفية لأفراد العينة، مثل: الجنس، المؤهل العلمي، وسنوات الخبرة. وقد تم استخدام الاختبارات الإحصائية المناسبة لهذه المتغيرات على النحو الآتي:

- اختبار: **T (T-test)** لفحص الفروق حسب الجنس (ذكر / أنثى)
- تحليل التباين الأحادي: **(One-Way ANOVA)** لفحص الفروق حسب كل من:
 - المؤهل العلمي دبلوم – بكالوريوس – ماجستير
 - سنوات الخبرة <5 سنوات، 5-10 سنوات، +10 سنوات

أظهرت نتائج التحليل أن جميع قيم **(P)** كانت أكبر من مستوى الدلالة **0.05**، وهو ما يدل على عدم وجود فروق ذات دلالة إحصائية في تقييم المشاركين لكفاءة إدارة المخاطر الإلكترونية، سواء بسبب الجنس أو المؤهل العلمي أو عدد سنوات الخبرة.

يشير هذا إلى أن استجابات المشاركين جاءت متقاربة نسبيًا، وأن إدراكهم لكفاءة إدارة المخاطر لا يتأثر بشكل كبير بخلفياتهم الديموغرافية أو المهنية، وهو ما يعكس توجهًا عامًا ومستقرًا في فهم وتطبيق ممارسات الحماية الرقمية داخل المؤسسات.

المتغير التصنيفي	قيمة p	نوع الاختبار	الدلالة
الجنس	0.4213	T-test	غير دالة
المؤهل العلمي	0.4930	ANOVA	غير دالة
سنوات الخبرة	0.2943	ANOVA	غير دالة

جدول 4.5 نتائج اختبار الفروق حسب الخصائص الشخصية والوظيفية

الفصل الخامس: مناقشة النتائج والتوصيات

5.1 المقدمة

يستعرض هذا الفصل نتائج الدراسة في ضوء أهدافها وتساؤلاتها وفروضها التي تم اختبارها في الفصل السابق، كما يناقش هذه النتائج مقارنة بما ورد في الدراسات السابقة والإطار النظري. ويهدف هذا الفصل إلى تفسير النتائج بشكل علمي دقيق، وربطها بالسياق الواقعي للمؤسسات السعودية والعربية فيما يتعلق بتوظيف التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية. كما يقدم الفصل مجموعة من التوصيات الذكية التي تستند إلى ما توصلت إليه الدراسة، بحيث تكون قابلة للتطبيق العملي وتساهم في تحسين مستوى الأمان السيبراني في المؤسسات المستهدفة.

5.2 النتائج المتعلقة بمتغيرات الدراسة الوصفية

أظهرت نتائج التحليل الوصفي للبيانات التي تم جمعها من عينة الدراسة ما يلي:

❖ الجنس:

تبين أن نسبة الذكور المشاركين كانت أعلى من الإناث، وهو ما يعكس تركيبة العاملين في أقسام تقنية المعلومات والأمن السيبراني في المؤسسات السعودية والعربية، حيث يغلب الطابع الذكوري على هذا المجال في معظم المؤسسات المستهدفة.

❖ الفئة العمرية:

تركزت أغلبية المشاركين ضمن الفئة العمرية (30-40 سنة)، ما يشير إلى أن معظم المتخصصين في تقنية المعلومات والأمن السيبراني ينتمون لفئة الشباب النشطين الذين يتمتعون بقدرة عالية على متابعة التطورات التقنية.

❖ المؤهل العلمي:

أظهرت النتائج ارتفاع نسبة الحاصلين على شهادة البكالوريوس، تليها الماجستير، وهو ما يؤكد توفر مستوى تأهيلي جيد لدى الكوادر العاملة في هذا المجال.

❖ سنوات الخبرة:

أوضحت النتائج أن أكثر من نصف المشاركين لديهم خبرة عملية تتراوح بين 5 إلى 10 سنوات في مجال تقنية المعلومات أو الأمن السيبراني، مما يعكس قدرة العينة على تقييم مدى فاعلية توظيف التكنولوجيا الحديثة بدقة.

❖ نوع المؤسسة:

بيّنت النتائج أن المؤسسات الحكومية أظهرت مستوى أعلى في تبني الحلول التقنية مقارنة ببعض المؤسسات الخاصة، مما قد يعزى إلى التزام المؤسسات الحكومية بالأنظمة والسياسات الوطنية للأمن السيبراني.

❖ حجم المؤسسة:

كشفت النتائج أن المؤسسات الكبيرة كانت الأكثر توظيفاً للتكنولوجيا الحديثة، بينما ظهرت تحديات أكبر في المؤسسات الصغيرة والمتوسطة تتعلق بالتكاليف ونقص الكفاءات المتخصصة.

5.3 النتائج المتعلقة باختبار فرضيات الدراسة

أسفر اختبار فروض الدراسة باستخدام الأساليب الإحصائية البارامترية عن نتائج هادفة تعزز أهمية توظيف التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية، وجاءت النتائج كما يلي:

❖ الفرضية الأولى:

أكدت النتائج وجود فروق ذات دلالة إحصائية بين المؤسسات التي توظف التكنولوجيا الحديثة وتلك التي لا توظفها في مستوى فعالية إدارة المخاطر الإلكترونية، لصالح المؤسسات التي تبنت الحلول التقنية. تعكس هذه النتيجة أهمية الاستثمار في التقنيات الحديثة لتعزيز قدرات الكشف المبكر والاستجابة السريعة للتهديدات.

❖ الفرضية الثانية:

كشفت النتائج عن علاقة ارتباط موجبة قوية بين مستوى توظيف التكنولوجيا الحديثة وفعالية إدارة المخاطر الإلكترونية. يشير هذا إلى أن زيادة استخدام الأنظمة الحديثة مثل الذكاء الاصطناعي وتقنيات التحليل التنبؤي يؤدي بشكل مباشر إلى رفع مستوى الأمان السيبراني في المؤسسات.

❖ الفرضية الثالثة:

أظهرت النتائج وجود فروق ذات دلالة إحصائية في فعالية إدارة المخاطر الإلكترونية تعزى لمتغير حجم المؤسسة، حيث كانت المؤسسات الكبيرة أكثر قدرة على تطبيق الحلول التقنية المتطورة مقارنة بالمؤسسات الصغيرة والمتوسطة، ما يعكس تأثير حجم الموارد والإمكانات المالية على مستوى الحماية.

❖ الفرضية الرابعة:

أكدت النتائج صحة الفرضية المتعلقة بوجود تحديات تنظيمية وبشرية تعيق توظيف التكنولوجيا الحديثة بفعالية، حيث اتفقت نسبة كبيرة من أفراد العينة على أن نقص الكوادر المؤهلة وصعوبة دمج الحلول التقنية مع الأنظمة الحالية تمثل أبرز العقبات.

مقارنة نتائج الدراسة الحالية بالدراسات السابقة

تتوافق نتائج هذه الدراسة بشكل كبير مع ما توصلت إليه دراسات سابقة تناولت توظيف التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية، وتحديدًا في البيئة السعودية والدولية، وذلك على النحو الآتي:

اسم الدراسة	أوجه الاتفاق أو الاختلاف مع الدراسة الحالية	النتائج الرئيسية	الهدف
Capgemini (2019)	تتفق النتائج مع دراستنا التي أظهرت استخدامًا واسعًا للذكاء الاصطناعي في التنبؤ بالتهديدات وتحليل السلوك الشبكي، مما يعزز فعالية الاستجابة.	ساهم في تقليل زمن الاكتشاف وخفض الإنذارات الكاذبة	استكشاف دور الذكاء الاصطناعي في الأمن السيبراني

اسم الدراسة	أوجه الاتفاق أو الاختلاف مع الدراسة الحالية	النتائج الرئيسية	الهدف
الغامدي (2022)	تتفق الدراسة في إبراز الحاجة إلى تدريب الكوادر، كما ظهر ذلك في محور التحديات المؤسسية.	ضعف تدريب الكوادر أبرز العوائق	تحليل تحديات الذكاء الاصطناعي في البيئة السعودية
ENISA (2021)	تتفق الدراسة مع نتائجنا في ضرورة التبني المبكر لتقنيات التحليل التنبؤي (Big Data + AI).	زيادة هجمات الفدية، والحاجة إلى الكشف المبكر	تحليل التهديدات السيبرانية على مستوى عالمي
آل هلال (2021)	تتفق النتائج مع دراستنا من حيث رصد فجوة بين الخطط والتطبيق، وضعف التنسيق المؤسسي الداخلي.	غياب استراتيجيات واضحة خاصة في الشركات الصغيرة	تقييم واقع إدارة المخاطر الإلكترونية في السعودية

جدول 5.1 مقارنة النتائج بالدراسات السابقة

5.4 التوصيات

استناداً إلى نتائج الدراسة وتحليل البيانات، تم التوصل إلى مجموعة من التوصيات الذكية التي يمكن أن تسهم في تحسين مستوى توظيف التكنولوجيا الحديثة لإدارة المخاطر الإلكترونية في المؤسسات السعودية والعربية، وهي:

(1) أولاً: تطوير خطط تدريبية متخصصة

تصميم وتنفيذ برامج تدريبية دورية تستهدف رفع كفاءة الموظفين في أقسام تقنية المعلومات والأمن السيبراني، مع التركيز على كيفية استخدام الأنظمة الحديثة مثل SIEM والتحليلات التنبؤية، على أن تُقيم هذه البرامج مرتين سنوياً وقياس أثرها من خلال اختبارات قبلية وبعدية لمستوى الوعي الأمني.

(2) ثانياً: تخصيص ميزانية مستقلة للأمن السيبراني

تخصيص نسبة لا تقل عن 5% من الميزانية التشغيلية السنوية للمؤسسة لدعم مشاريع تطوير البنية التحتية للأمن السيبراني وتبني الحلول التقنية المتقدمة، ومراجعة هذه النسبة سنوياً بناءً على مستجدات التهديدات الإلكترونية.

(3) ثالثاً: تحديث السياسات والإجراءات الأمنية

مراجعة وتحديث سياسات وإجراءات أمن المعلومات بشكل دوري (مرة كل 12 شهراً على الأقل) لتتوافق مع التغيرات في طبيعة التهديدات الإلكترونية، وإشراك جميع الإدارات ذات العلاقة في هذه المراجعة لضمان الالتزام الكامل بالتحديثات.

(4) رابعاً: تعزيز التكامل بين الأنظمة التقنية

العمل على دمج الأنظمة الأمنية الحديثة مع بقية الأنظمة التقنية المستخدمة في المؤسسة، مثل نظم إدارة الموارد ERP، لتوحيد مصادر البيانات وتسهيل اكتشاف التهديدات وتحليلها بشكل متكامل.

5) خامساً: التعاون مع جهات متخصصة

إبرام اتفاقيات شراكة مع الشركات المزودة لحلول الأمن السيبراني والهيئات الوطنية المختصة، مثل الهيئة الوطنية للأمن السيبراني، للاستفادة من خبراتها وخدماتها في تحسين البنية التحتية الأمنية للمؤسسات.

6) سادساً: التوعية المستمرة لجميع الموظفين

تنظيم حملات توعية ربع سنوية لجميع الموظفين حول مخاطر الأمن السيبراني، وأهمية الالتزام بسياسات الاستخدام الآمن للأجهزة والبريد الإلكتروني، وقياس نسبة التحسن في وعي الموظفين من خلال استبيانات دورية.

Abstract

This study aims to analyze the role played by modern technology in enhancing cyber risk management within Saudi and Arab institutions by examining the extent to which these institutions adopt advanced technologies such as artificial intelligence and big data analytics, as well as their ability to effectively detect and respond to cyber threats. The significance of this study arises from the urgent need to strengthen cybersecurity measures in organizations to address the increasing complexity of cyber threats, which can severely impact business continuity and institutional reputation.

The study adopted the descriptive analytical method, and a comprehensive electronic questionnaire was designed and distributed to a sample of 250 employees working in IT and cybersecurity departments in both public and private institutions of various sizes. Data were analyzed using descriptive and inferential statistical methods, including T-tests, one-way ANOVA, and correlation analysis, while data validity was ensured through normality tests and reliability analysis.

The study results revealed a strong, statistically significant positive correlation between the level of modern technology adoption and the effectiveness of cyber risk management. The results also showed significant differences attributed to the institution size, with larger organizations demonstrating higher efficiency in cyber risk management compared to small and medium-sized enterprises. Furthermore, the findings indicated that key challenges hindering effective technology adoption include human and organizational barriers, such as the lack of qualified personnel and difficulties integrating advanced solutions with existing systems.

The study recommended developing periodic specialized training plans for cybersecurity staff, allocating independent budgets for cybersecurity initiatives, regularly updating security policies, enhancing integration among different technological systems, and collaborating with national cybersecurity authorities to achieve comprehensive and effective protection of institutional digital assets and ensure business continuity in light of growing cyber threats.

Keywords:

Cybersecurity, Cyber Risk Management, Modern Technology, Artificial Intelligence, Saudi Institutions, Technological Solutions.

المراجع

قائمة المراجع العربية

1. الهيئة الوطنية للأمن السيبراني. (2022). *السياسات الوطنية للأمن السيبراني*. الرياض: المملكة العربية السعودية.
2. المنظمة العربية لتكنولوجيات الاتصال والمعلومات. (2021). *التحديات السيبرانية في العالم العربي*. تونس: المنظمة العربية.
3. لجنة الأمم المتحدة الاقتصادية والاجتماعية لغرب آسيا (الإسكوا). (2020). *الأمن السيبراني والتحول الرقمي في الدول العربية*. بيروت: الأمم المتحدة.
4. عبد الله، خالد بن محمد. (2021). أثر توظيف التكنولوجيا الحديثة في تحسين استراتيجيات الأمن السيبراني في المؤسسات السعودية *مجلة الدراسات الأمنية السعودية*، 15(2)، 58.33-.
5. يوسف، سامي عبد الرحمن. (2020). أثر الوعي السيبراني في حماية المؤسسات من الهجمات الإلكترونية. *المجلة العربية للأمن المعلوماتي*، 8(1)، 47.21-.
6. العمري، علي بن سعيد. (2022). معوقات تطبيق التقنيات الحديثة في إدارة المخاطر الإلكترونية بالقطاع الحكومي السعودي *مجلة الإدارة العامة*، 62(1)، 112.87-.
7. مركز الخليج للأبحاث. (2021). *الأمن السيبراني في دول الخليج: الواقع والتحديات*. جدة: مركز الخليج للأبحاث.
8. الخطيب، مروان. (2019). أثر الحوكمة الإلكترونية على تحسين إدارة المخاطر في المؤسسات العربية *مجلة الاقتصاد والإدارة*، 25(3)، 12899-.

قائمة المراجع الإنجليزية

9. Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.
10. ENISA. (2021). *ENISA Threat Landscape 2021*. European Union Agency for Cybersecurity. Retrieved from <https://www.enisa.europa.eu>
11. ISO/IEC. (2018). *ISO/IEC 27001: Information security management systems – Requirements*. International Organization for Standardization.

- 12.Kshetri, N. (2019). The emerging role of big data in key development issues: Opportunities, challenges, and concerns. In *Big Data for Development* (pp. 1–36).
- 13.Sharma, S., & Sahay, S. K. (2021). Machine learning for cybersecurity: A comprehensive survey. *IEEE Access*, 9, 132286–132325.
- 14.Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102.
- 15.Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, 78, 544–546.
- 16.Alasmary, W., & Alhaidari, F. (2020). A review on cybersecurity challenges and solutions in Saudi Arabia. *International Journal of Advanced Computer Science and Applications*, 11(6), 125–130.
- 17.Lemos, R. (2018). The evolution of ransomware. *IEEE Security & Privacy*, 16(4), 68–71.
- 18.Hentea, M., Dhillon, H. S., & Dhillon, M. (2006). Towards changes in information security education. *Journal of Information Technology Education: Research*, 5, 221–233.
- 19.Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., & Almomani, E. (2013). A survey of phishing email filtering techniques. *IEEE Communications Surveys & Tutorials*, 15(4), 2070–2090.
- 20.Raghavan, S., & Parthiban, L. (2014). The cyber security landscape in the Middle East. *International Journal of Computer Applications*, 93(16), 1–5.

استمارة الاستبيان

عنوان الدراسة:

دور التكنولوجيا الحديثة في تحسين إدارة المخاطر الإلكترونية وأساليب الحماية

عزيزتي/عزيزي المشارك/ة،

تهدف هذه الاستبانة إلى جمع آراء العاملين في قطاعات تقنية المعلومات والأمن السيبراني حول مدى استخدام التكنولوجيا الحديثة في إدارة المخاطر الإلكترونية. نأمل تعبئة الاستبانة بكل موضوعية ودقة، علمًا بأن جميع المعلومات ستستخدم لأغراض البحث العلمي فقط.

أولاً: البيانات الشخصية والوظيفية

1. الجنس:

☐ ذكر

☐ أنثى

2. الفئة العمرية:

☐ أقل من 30 سنة

☐ 30 - أقل من 40 سنة

☐ 40 - أقل من 50 سنة

☐ 50 سنة فأكثر

3. المؤهل العلمي:

☐ دبلوم

☐ بكالوريوس

☐ ماجستير فأعلى

4. سنوات الخبرة:

☐ أقل من 5 سنوات

☐ من 5 إلى أقل من 10 سنوات

☐ 10 سنوات فأكثر

ثانيًا: محاور الاستبانة (مقياس ليكرت الخماسي)

= 1 لا أوافق بشدة، 2 = لا أوافق، 3 = محايد، 4 = أوافق، 5 = أوافق بشدة

المحور الأول: توظيف الذكاء الاصطناعي في إدارة المخاطر الإلكترونية

البيان	1	2	3	4	5
تستخدم مؤسستي أدوات ذكاء اصطناعي لاكتشاف الهجمات الإلكترونية.	☐	☐	☐	☐	☐
يتم تحليل السلوك الشبكي المشبوه باستخدام الذكاء الاصطناعي.	☐	☐	☐	☐	☐
يستخدم الذكاء الاصطناعي في التنبؤ بالتهديدات المستقبلية.	☐	☐	☐	☐	☐
يعتمد قسم الأمن السيبراني على التعلم الآلي في تقليل زمن الاستجابة.	☐	☐	☐	☐	☐
يوجد استثمار مستمر في تقنيات الذكاء الاصطناعي لأغراض الحماية.	☐	☐	☐	☐	☐

المحور الثاني: تحليلات البيانات الضخمة Big Data Analytics

البيان	1	2	3	4	5
تعتمد المؤسسة على تحليل بيانات ضخمة لرصد التهديدات الأمنية.	☐	☐	☐	☐	☐
يتم تتبع أنماط التهديدات عبر منصات التحليل المتقدم.	☐	☐	☐	☐	☐
نُمكننا البيانات من اتخاذ قرارات استباقية ضد المخاطر.	☐	☐	☐	☐	☐
توجد بنية تحتية متقدمة لمعالجة البيانات الضخمة في المؤسسة.	☐	☐	☐	☐	☐
تحليل البيانات يساهم في تعزيز استجابة المؤسسة للهجمات السيبرانية.	☐	☐	☐	☐	☐

المحور الثالث: أنظمة أمن المعلومات

البيان	1	2	3	4	5
تمتلك المؤسسة نظامًا موثوقًا لإدارة أمن المعلومات (ISMS).	☐	☐	☐	☐	☐
يتم تحديث أنظمة الحماية والرقابة بشكل دوري.	☐	☐	☐	☐	☐
هناك التزام واضح بسياسات أمن المعلومات بين الموظفين.	☐	☐	☐	☐	☐
يتم إجراء تدقيقات داخلية دورية على أنظمة المعلومات.	☐	☐	☐	☐	☐
تمتلك المؤسسة خطة استجابة للطوارئ الإلكترونية.	☐	☐	☐	☐	☐

المحور الرابع: الاستجابة للحوادث السيبرانية

البيان	1	2	3	4	5
توجد وحدة مختصة للتعامل مع الحوادث الإلكترونية داخل المؤسسة.	☐	☐	☐	☐	☐
يتم تدريب الموظفين على خطط الاستجابة للأزمات السيبرانية.	☐	☐	☐	☐	☐
يتم توثيق وتحليل كل حادثة إلكترونية للاستفادة منها لاحقًا.	☐	☐	☐	☐	☐
يوجد نظام لإخطار الجهات المختصة فور وقوع حادثة إلكترونية.	☐	☐	☐	☐	☐
الاستجابة للحوادث تتم وفق بروتوكول زمني محدد مسبقًا.	☐	☐	☐	☐	☐

المحور الخامس: التحديات المؤسسية

البيان	1	2	3	4	5
توجد مقاومة داخلية تجاه التغيير الرقمي في المؤسسة.	☐	☐	☐	☐	☐
ضعف ميزانية الأمن السيبراني يعيق التطوير التقني.	☐	☐	☐	☐	☐
نقص الكوادر البشرية المؤهلة في مجال التقنية.	☐	☐	☐	☐	☐
وجود فجوة بين الخطط التقنية والتطبيق الفعلي.	☐	☐	☐	☐	☐

Midocean University

College of Management



Department/ Major in Risk Management

**The Role of modern Technology in Improving Risk and
Electronic Threat Management Processes and Protection
Methods.**

Prepared by the Student/

Sarah Ahmed Al-Qahtani

(243001145)

Supervised/

Dr. Al-Faisal Abdul Hamid Mohammed Hassan

Dr. Fayez Jarad

2024-2025