

جامعة ميد أوشن



كلية الإدارة

ماجستير إدارة المخاطر للخريجين

أثر إدارة مخاطر العامل البشري على الحد من الهجمات السيبرانية:
دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية

إعداد الطالب/

وليد نبيل القباني

2021201871

إشراف/

د. الفيصّل عبد الحميد محمد حسن

العام الدراسي:

2025 – 1447

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



أهدي هذا العمل إلى والديّ الكريمين، اللذين كانا لي النبراس والداعم الأكبر في حياتي. إلى والدتي الحنونة، التي غرست فيّ حب العلم والمعرفة، وإلى والدي العزيز، الذي علمني قوة الإرادة والمثابرة.

إلى زوجتي العزيزة، التي كانت لي الشريك المخلص والداعم في كل مرحلة من مراحل هذه الرحلة، أهدي هذا الإنجاز كتقدير وامتنان لدعمها وصبرها اللامحدود.

إلى أساتذتي الأفاضل، الذين لم يخلوا عليّ بعلمهم وتوجيهاتهم. كان لخبرتهم وإرشاداتهم الأثر الكبير في إنجاز هذا العمل.

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

وأخيرًا، أهدي هذا العمل إلى كل من ساهم في دعمي وشجعني، سائلًا الله أن يجعل هذا الإنجاز بداية لمزيد من النجاحات والتقدم.

شُكْرُوتَكَ

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

أتقدم بخالص الشكر والتقدير إلى والديّ العزيزين، اللذين كانا لي الدعم الأكبر والأساس في كل مراحل حياتي. إن إيمانهما بي ودعمهما المتواصل كانا الدافع وراء هذا الإنجاز.

كما أعبر عن عميق امتناني لزوجتي الغالية، التي كانت لي الشريك والسند في هذه الرحلة. كان لتفهمها ودعمها وصبرها دور كبير في تحقيق هذا العمل.

أشكر أساتذتي الأفاضل، وبالأخص مشرفي الكريم، على توجيهاتهم السديدة وإرشاداتهم القيمة التي ساعدتني على تطوير هذا البحث وإتمامه بنجاح.

د. الفيصل عبد الحميد محمد

أود أيضًا أن أشكر زملائي وأصدقائي، الذين كانوا لي خير رفاق وداعمين، وشاركوا معي التحديات والنجاحات. إن دعمهم وتشجيعهم كان لهما 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. أسأل الله أن يوفقنا جميعًا لما فيه الخير، وأن يجعل هذا العمل نافعًا ومثمرًا.

المستخلص

تهدف الدراسة إلى معرفة مدى أثر تطبيق إدارة مخاطر العامل البشري بأبعادها مجمعة المتمثلة في (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد من الهجمات السيبرانية: دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية ، تم اتباع المنهج الوصفي التحليلي، تم توزيع الاستبانة على عينة عشوائية من العاملين في البنوك الحكومية بمدينة الرياض، وقد بلغ عدد الاستبانات الصالحة للتحليل (350) استبانة، استخدم الباحث مجموعة من الأساليب الإحصائية لتحليل البيانات.

أظهرت نتائج الدراسة وجود مستوى مرتفع جدا من تحديد وتقييم المخاطر كأحد ابعاد إدارة مخاطر العامل البشري ، و وجود مستوى مرتفع جدا من معالجة إدارة المخاطر كأحد ابعاد إدارة مخاطر العامل البشري

وفي ضوء النتائج، توصي الدراسة بتعزيز برامج التوعية الأمنية المستمرة لجميع الموظفين، مع التركيز على التهديدات السيبرانية المرتبطة بالسلوك البشري كالهندسة الاجتماعية والتصيد الإلكتروني ، تضمين إدارة مخاطر العامل البشري ضمن الخطة الاستراتيجية للأمن السيبراني في المؤسسات الحكومية لضمان معالجة التهديدات البشرية بشكل منهجي.

الكلمات المفتاحية: مخاطر العامل البشري – الهجمات السيبرانية – المؤسسات الحكومية

قائمة المحتويات

أ.....	بسم الله الرحمن الرحيم
ب.....	الإهداء
ج.....	الشكر والتقدير
د.....	المستخلص
ه.....	قائمة المحتويات
ط.....	قائمة الجداول
ي.....	قائمة الأشكال
1.....	الفصل الأول: الإطار العام للدراسة
1.....	1.1 المقدمة
4.....	2.1 أهمية الدراسة
4.....	1.2.1 الأهمية النظرية
5.....	2.2.1 الأهمية العملية
5.....	3.1 أهداف الدراسة
6.....	4.1 تساؤلات الدراسة
6.....	5.1 فروض الدراسة
7.....	6.1 نموذج الدراسة
7.....	7.1 دراسات سابقة
14.....	8.1 الفجوة البحثية
16.....	9.1 المنطلقات النظرية للدراسة
18.....	10.1 المنهجية وطرق البحث
19.....	11.1 مصادر جمع البيانات
19.....	12.1 أدوات الدراسة

13.1	الأساليب الإحصائية المستخدمة	19
14.1	أداة الدراسة	20
15.1	حدود الدراسة	20
	الفصل الثاني: الإطار النظري	22
	المبحث الأول: فهم العوامل البشرية وتشرح الأخطاء النظامية	22
1.1.2	المقدمة	22
2.1.2	الهندسة البشرية وتصميم بيئة العمل الآمنة	22
3.1.2	إدماج المخاطر البشرية في منظومة إدارة المخاطر المؤسسية	24
4.1.2	التنوع والشمولية كصمام أمان سلوكي	25
5.1.2	هندسة "النقطة الحمراء" واستباق الخطأ السريري	25
6.1.2	الذكاء الثقافي وإدارة مخاطر القوى العاملة متعددة الجنسيات	26
7.1.2	نظريات "التعويض الخطر" ومواجهة ميل الأفراد إلى الاستهتار	28
8.1.2	إيقاع المناوبات الذكية وإنصاف الساعة البيولوجية	29
9.1.2	المؤشرات القائدة في السلامة مقابل المؤشرات التابعة	30
10.1.2	استراتيجيات التصحيح الفوري ونافذة الذهب	31
11.1.2	الكشف المبكر عن "مستودعات الغضب" بين الفرق	33
12.1.2	دراسة "الحوادث الإيجابية" ورصد النجاح المنقذ	35
13.1.2	الذكاء الاصطناعي في خدمة الحد من الأخطاء البشرية	38
	المبحث الثاني: الهجمات السيبرانية	39
1.2.2	المقدمة	39
2.2.2	تنامي دور التأمين السيبراني والخلاف حول جدواه	46
3.2.2	الهندسة العكسية للهجمات ودورها في تطوير أساليب الحماية	48
	الفصل الثالث: منهجية وإجراءات الدراسة	54
1.3	مقدمة	54

54.....	2.3 منهجية البحث:
54.....	3.3 مجتمع وعينة الدراسة.....
54.....	4.3 مصادر جمع البيانات والمعلومات:
55.....	5.3 الأساليب الإحصائية:
55.....	6.3 أداة الدراسة.....
56.....	7.3 صدق أداة الدراسة.....
56.....	المحور الأول: إدارة مخاطر العامل البشري
58.....	المحور الثاني: الحد من الهجمات السيبرانية
60.....	8.3 ثبات أداة الدراسة:
61.....	الفصل الرابع: تحليل النتائج.....
61.....	1.4 مقدمة.....
61.....	2.4 خصائص عينة الدراسة.....
62.....	3.4 تحليل استمارة الاستبيان.....
62.....	المحور الأول: إدارة مخاطر العامل البشري
65.....	المحور الثاني: الحد من الهجمات السيبرانية
67.....	3.4 اختبار فروض الدراسة.....
71.....	الفصل الخامس: النتائج والتوصيات والمقترحات.....
71.....	1.5 مقدمة.....
71.....	2.5 نتائج الدراسة.....
73.....	3.5 التوصيات.....
74.....	4.5 المقترحات.....
76.....	Abstract.....
77.....	قائمة المراجع.....
77.....	أولا: المراجع باللغة العربية.....

79.....	ثانيا: المراجع باللغة الإنجليزية
85.....	الملاحق
86.....	استمارة استبيان

قائمة الجداول

رقم الجدول	اسم الجدول	رقم الصفحة
1.	جدول (1) مستويات موافقة عينة الدراسة على عبارات أداة الدراسة	56
2.	جدول (2) معاملات الارتباط لعبارات المحور الاول	57
3.	جدول (3) معاملات الارتباط لعبارات المحور الثاني	59
4.	جدول (4) معامل الثبات لمحاو استمارة الاستبيان	60
5.	جدول (5) توزيع عينة الدراسة وفقا لخصائصها	61
6.	جدول (6) المتوسط الحسابي والانحراف المعياري والترتيب ومستوي الموافقة على عبارات تحديد وتقييم المخاطر	62
7.	جدول (7) المتوسط الحسابي والانحراف المعياري والترتيب ومستوي الموافقة على عبارات معالجة إدارة المخاطر	63
8.	جدول (8) المتوسط الحسابي والانحراف المعياري والترتيب ومستوي الموافقة على عبارات مراقبة إدارة المخاطر	64
9.	جدول (9) المتوسط الحسابي والانحراف المعياري والترتيب ومستوي الموافقة على عبارات الحد من الهجمات السيبرانية	66
10.	جدول (10) نتائج نموذج الانحدار الخطي البسيط لأثر إدارة مخاطر العامل البشري على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية	67
11.	جدول (11) نتائج نموذج الانحدار الخطي البسيط لأثر تحديد وتقييم المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية	69

رقم الصفحة	اسم الجدول	رقم الجدول
70	جدول (12) نتائج نموذج الانحدار الخطي البسيط لأثر معالجة إدارة المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية	12.
71	جدول (13) نتائج نموذج الانحدار الخطي البسيط لأثر مراقبة إدارة المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية	13.

قائمة الأشكال

رقم الصفحة	اسم الجدول	رقم الجدول
7	الشكل رقم (1) متغيرات الدراسة	1.

الفصل الأول: الإطار العام للدراسة

1.1 المقدمة

تُعد إدارة المخاطر عنصراً أساسياً يلعب دوراً حيوياً في نجاح المؤسسات الحديثة، إذ تُساهم في تحقيق الأهداف الاستراتيجية وتعزيز القدرة التنافسية. تتضمن إدارة المخاطر تحديد المخاطر المحتملة وتقييمها ووضع الخطط المناسبة لمواجهتها، مما يُساعد على تقليل الآثار السلبية التي قد تؤثر على الأداء العام للمؤسسة. (سلمونة، 2024)

تبدأ عملية إدارة المخاطر بتحديد أنواع المخاطر المختلفة التي قد تواجهها المؤسسة، سواءً كانت مالية أو تشغيلية أو استراتيجية أو حتى بيئية. ومن خلال هذه العملية، يُمكن للمؤسسات توقع التحديات المحتملة ووضع استراتيجيات فعالة للتخفيف من آثارها. على سبيل المثال، قد تشمل المخاطر المالية تقلبات السوق أو تغيرات أسعار المواد الخام، بينما قد تشمل المخاطر التشغيلية مشاكل سلسلة التوريد أو عدم الكفاءة التشغيلية. (العنبرية، 2023)

بعد تحديد المخاطر، تأتي المرحلة التالية وهي تقييمها. يتطلب ذلك تحليل مدى تأثير كل خطر على المؤسسة واحتمالية حدوثه. يُساعد هذا التحليل على تخصيص الموارد بفعالية أكبر، حيث يُمكن للمؤسسات التركيز على المخاطر الأكثر تأثيراً واحتمالية، مما يُعزز فعالية استراتيجيات التخفيف من آثارها. تتطلب إدارة المخاطر أيضاً توعية الموظفين وتثقيفهم، إذ يلعب كل فرد داخل المؤسسة دوراً في تحديد المخاطر والاستجابة لها على النحو المناسب. ومن خلال بناء ثقافة مؤسسية تُعزز أهمية إدارة المخاطر، يُمكن للمؤسسات المساهمة في تعزيز المرونة والقدرة على الاستجابة السريعة للتغيرات والضغط الخارجي. (القحطاني، 2023)

إدارة المخاطر ليست مجرد عملية روتينية، بل هي عنصر أساسي لاستدامة الأعمال ونجاحها في بيئة عمل معقدة ومتغيرة باستمرار. ومن خلال استراتيجيات فعالة لإدارة المخاطر، لا تستطيع المؤسسات حماية نفسها من التهديدات فحسب، بل أيضاً اغتنام فرص جديدة للنمو والتوسع. (المري، 2020)

يُعدّ العامل البشري أحد أهم العناصر في أي مؤسسة، إذ يلعب دورًا حيويًا في تشكيل نجاحها وفعاليتها. فالموظفون ليسوا مجرد أدوات تشغيلية، بل هم المحرك الرئيسي الذي يُسهم في تحقيق الأهداف الاستراتيجية للمؤسسة. ويتجلى تأثير العامل البشري في جوانب عديدة، منها الإبداع والتفاعل والتكيف مع التغيير، مما يُسهم بشكل مباشر في تحسين الأداء العام للمؤسسة. (باقر، 2020)

ومن الجوانب الأساسية لتأثير العامل البشري القدرة على الإبداع والابتكار. فالأفراد ذوو المهارات والخلفيات الثقافية المتنوعة قادرون على تقديم أفكار جديدة وحلول مبتكرة للمشكلات. وهذا التنوع في التفكير يُعزز قدرة المؤسسة على المنافسة في الأسواق المتغيرة، ويُساهم في تطوير منتجات وخدمات جديدة تُلبّي احتياجات العملاء بشكل أفضل. لذلك، يُصبح الاستثمار في تطوير مهارات الموظفين وتعزيز ثقافة الابتكار أمرًا أساسيًا لضمان استمرار النجاح. (الحسني، 2022)

علاوة على ذلك، يلعب التفاعل الشخصي داخل مكان العمل دورًا محوريًا في تعزيز التواصل والتعاون. فعندما يتمتع الموظفون ببيئة عمل تُشجع على المشاركة الفعالة وتبادل الأفكار، يُسهم ذلك في بناء علاقات قوية تُعزز روح الفريق. تساعد هذه الروح التعاونية على تحسين الكفاءة وتقليل الأخطاء، حيث يعمل الأفراد معًا لتحقيق أهداف مشتركة. كما يعكس تعزيز العلاقات الإنسانية في العمل التزام المؤسسة برفاحية موظفيها، مما يؤثر إيجابًا على الإنتاجية والرضا الوظيفي. (الرواشدة، 2022)

تُعد القدرة على التكيف مع التغيير عاملًا بشريًا مهمًا أيضًا. ففي عالم سريع التغير، تحتاج المؤسسات إلى أفراد قادرين على مواجهة التحديات الجديدة والتكيف مع الظروف المتغيرة. فالموظفون الذين يتمتعون بالمرونة العقلية والقدرة على التعلم السريع قادرون على الاستجابة بفعالية للابتكارات التكنولوجية وتقلبات الأسواق. ولا يقتصر هذا التكيف على الحفاظ على استقرار المؤسسة فحسب، بل يعزز أيضًا قدرتها على استكشاف فرص جديدة. (أبو نصر، 2020)

لا يمكن الاستهانة بأهمية العامل البشري في تحقيق النجاح المؤسسي. فالاستثمار في تطوير مهارات موظفيهم وتعزيز بيئة عمل إيجابية يساهم في تحسين الأداء العام والابتكار. لذلك، يُعد فهم وتقدير قيمة

العامل البشري خطوة أساسية نحو بناء مؤسسات قوية ومستدامة قادرة على مواجهة تحديات المستقبل بثقة. (الشوكة، 2020)

تُعدّ الهجمات الإلكترونية من أبرز التحديات التي تواجه المؤسسات والأفراد في العصر الرقمي الحديث، مع تزايد تهديدات الأمن الإلكتروني بوتيرة متسارعة. تعتمد هذه الهجمات على استغلال ثغرات الأنظمة والشبكات، مما يُعرض البيانات الحساسة للخطر، ويُلحق الضرر بسمعة الشركات وعملياتها التشغيلية. يُعدّ الفهم العميق لطبيعة هذه الهجمات وأبعادها أمرًا بالغ الأهمية لحماية المعلومات والموارد الحيوية. (عوض، 2022)

تتراوح الهجمات الإلكترونية بين البرمجيات الخبيثة، وهجمات رفض الخدمة، والاحتيال الإلكتروني، ولكل منها تأثيرها الفريد على الأفراد والمؤسسات. على سبيل المثال، يُمكن للبرمجيات الخبيثة تسريب بيانات حساسة، بينما يُمكن لهجمات رفض الخدمة تعطيل الخدمات الإلكترونية والتأثير على قدرة المؤسسة على العمل بسلاسة. تزداد هذه التهديدات تعقيدًا مع تطور التكنولوجيا، حيث يستخدم المهاجمون تقنيات متقدمة لتجاوز أنظمة الأمن التقليدية. (الرواشدة، 2022)

تتنوع الدوافع وراء الهجمات الإلكترونية، ويمكن أن تكون اقتصادية، أو سياسية، أو حتى شخصية. يسعى بعض المهاجمين إلى تحقيق مكاسب مالية من خلال سرقة البيانات أو ابتزاز المؤسسات، بينما قد يسعى آخرون إلى إحداث تأثير سياسي أو اجتماعي. لذا، أصبح من الضروري للمؤسسات وضع استراتيجيات شاملة لمواجهة هذه التهديدات وفهم طبيعة المخاطر التي قد تواجهها. (المقدشي، 2019)

تُعدّ التدابير الوقائية جزءًا لا يتجزأ من استراتيجية الأمن السيبراني. ويتطلب ذلك استخدام تقنيات متقدمة مثل التشفير وجدران الحماية وأنظمة كشف التسلل، بالإضافة إلى توعية الموظفين بأهمية الأمن السيبراني. فبينما يُعدّ البشر ثروة قيّمة، إلا أنهم قد يُشكّلون أيضًا نقطة ضعف إذا لم يتلقوا التدريب المناسب للتعرف على التهديدات والتصدي لها. (العمرى، 2022)

تُمثّل الهجمات السيبرانية تحديًا مستمرًا يتطلب تضافر جهود جميع الجهات المعنية، بما في ذلك الحكومات والمؤسسات والأفراد. ويُعدّ التوعية بأهمية الأمن السيبراني ووضع استراتيجيات فعّالة لمواجهة

هذه التهديدات خطوةً أساسيةً نحو حماية المعلومات والموارد الحيوية في عالمٍ متزايد الترابط. (الصمادي، 2023)

2.1 أهمية الدراسة

تعتمد أهمية هذه الدراسة على إسهاماتها النظرية والتطبيقية فيما يلي:

1.2.1 الأهمية النظرية

- ✓ تتناول الدراسة موضوعًا مترابطًا يجمع بين مفاهيم إدارة المخاطر والسلوك البشري والأمن السيبراني. يُعدّ هذا التكامل نادرًا نسبيًا في الأدبيات الأكاديمية العربية، التي غالبًا ما تُركّز على الجوانب التقنية دون تناول كافٍ للبعد الإنساني للتهديدات السيبرانية.
- ✓ تُسهم الدراسة في تطوير إطار نظري جديد لفهم سلوك الأفراد داخل المؤسسات كعناصر فاعلة في منظومة التهديدات. ويتحقق ذلك من خلال تحليل العوامل المؤدية إلى الأخطاء الأمنية (مثل نقص الوعي أو الإهمال أو الجهل باللوائح الأمنية)، واقتراح آليات لإدارة هذا النوع من المخاطر ضمن منظومة أمن الشركات.
- ✓ تُساعد الدراسة على سد فجوة معرفية تتعلق بغياب التكامل الواضح بين الأدبيات التي تتناول إدارة المخاطر كوظيفة إدارية ونظريات السلوك التنظيمي التي تُفسر سلوك الأفراد في مكان العمل، لا سيما فيما يتعلق بمواجهة التهديدات السيبرانية الحديثة.
- ✓ يفتح هذا البحث المجال أمام باحثين آخرين لتطوير أدوات قياس كمية ونوعية لتقييم وعي الأفراد بالمخاطر السيبرانية والتزامهم بالإجراءات الوقائية، وربط ذلك بالنتائج الأمنية كعدد الحوادث أو معدل التفاعل مع رسائل التصيد الاحتيالي، مما يعزز الأساس العلمي في هذا المجال.
- ✓ يُثري البحث المكتبة العربية بإضافة نظرية جديدة باللغة العربية في مجال معاصر وحساس للغاية، مما يُسهم في رفع الوعي البحثي والتطبيقي للأمن السيبراني من منظور إنساني في السياق العربي.

2.2.1 الأهمية العملية

- ✓ تُبرز الدراسة الدور المحوري للعامل البشري كأحد أكثر نقاط الضعف شيوعاً في أنظمة الأمن السيبراني. وتُشير التقارير إلى أن نسبة كبيرة من الهجمات الناجحة تُنفذ باستغلال السلوك البشري الخاطئ، مما يجعل معالجة هذه المخاطر ضرورةً تنظيميةً وليست خياراً.
- ✓ تُقدم الدراسة خارطة طريق عملية للمؤسسات لتحديد السلوكيات البشرية المحفوفة بالمخاطر (مثل ضعف الوعي الأمني، والاستجابة المتهورة لرسائل التصيد الاحتيالي، ومشاركة كلمات المرور)، وتُقدِّم تدخلات إدارية مثل التدريب والتوعية وسياسات الرقابة التي من شأنها الحد من احتمالية التعرض للاختراقات.
- ✓ تُساعد الدراسة في توجيه صانعي القرار نحو تبني سياسات أمن سيبراني أكثر شمولاً تتجاوز الأدوات التقنية، لتشمل أيضاً إدارة رأس المال البشري، ووضع برامج توعية دورية، وتقييم الأداء الفردي في التعامل مع المواقف الأمنية، مما يُعزز جاهزية المؤسسات.
- ✓ تُوفر الدراسة إطار عمل يُمكن تطبيقه في القطاعات الحساسة (مثل المالية والحكومة والتعليم والطاقة)، وهي من أكثر القطاعات استهدافاً للهجمات السيبرانية. يُساهم هذا الإطار في تعزيز أمن المعلومات على المستويين الوطني والمؤسسي.
- ✓ تُساعد الدراسة في تقليل الخسائر المالية والتشغيلية الناتجة عن نقاط الضعف البشرية، سواءً المتعلقة بتعطيل النظام أو تسرب البيانات أو الإضرار بسمعة الشركات، من خلال تقديم توصيات قابلة للتطبيق في بيئات العمل الرقمية الحالية.

3.1 أهداف الدراسة

- تهدف الدراسة إلى معرفة مدى أثر تطبيق إدارة مخاطر العامل البشري بأبعادها مجمعة المتمثلة في (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد من الهجمات السيبرانية: دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية، ويتفرع منه مجموعة من الأهداف الفرعية:

- ✓ التعرف على تحديد وتقييم المخاطر ومدى انعكاسها على الحد من الهجمات السيبرانية.
- ✓ التعرف على معالجة إدارة المخاطر ومدى انعكاسها على الحد من الهجمات السيبرانية.
- ✓ التعرف على مراقبة إدارة المخاطر ومدى انعكاسها على الحد من الهجمات السيبرانية.

4.1 تساؤلات الدراسة

السؤال الرئيسي الأول: ما أثر تطبيق إدارة مخاطر العامل البشري بأبعادها مجمعة المتمثلة في (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد من الهجمات السيبرانية: دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية، وتتفرع منه عدة أسئلة فرعية كالتالي:

- ✓ ما أثر التعرف على تحديد وتقييم المخاطر ومدى انعكاسها على الحد من الهجمات السيبرانية؟
- ✓ ما أثر التعرف على معالجة إدارة المخاطر ومدى انعكاسها على الحد من الهجمات السيبرانية؟
- ✓ ما أثر التعرف على مراقبة إدارة المخاطر ومدى انعكاسها على الحد من الهجمات السيبرانية؟

5.1 فروض الدراسة:

لتحقيق أهداف الدراسة والإجابة على تساؤلاتها يمكن للباحث اعتماداً على الإطار النظري المتعلق بالدراسة، واستناداً إلى نتائج الدراسات السابقة تم صياغة الفرضيات التالية:

الفرضية الرئيسة الأول: لا يوجد أثر ذو دلالة إحصائية لتطبيق إدارة مخاطر العامل البشري بأبعادها مجمعة المتمثلة في (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد من الهجمات السيبرانية: دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية

وينبثق من هذه الفرضية الفرضيات الفرعية الثلاث التالية:

- ✓ لا يوجد أثر ذو دلالة إحصائية تحديد وتقييم المخاطر ومدى انعكاسها على الحد من الهجمات السيبرانية

✓ لا يوجد أثر ذو دلالة إحصائية ل معالجة إدارة المخاطر ومدى انعكاسها على الحد من الهجمات السيبرانية

✓ لا يوجد أثر ذو دلالة إحصائية لمراقبة إدارة المخاطر ومدى انعكاسها على الحد من الهجمات السيبرانية

6.1 نموذج الدراسة:

- المتغير المستقل: إدارة مخاطر العامل البشري بأبعادها مجمعة المتمثلة في (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر)
- المتغير التابع: الهجمات السيبرانية

الشكل رقم (1) متغيرات الدراسة



7.1 دراسات سابقة

1. دراسة حلول (2019) بعنوان: إدارة المخاطر في شركات التأمين: دراسة حالة الشركة الوطنية

للتأمين SAA وكالة غليزان للفترة "2016-2014"

تهدف هذه الدراسة المتواضعة إلى تسليط الضوء على الأساليب المختلفة التي تتبعها شركات التأمين لإدارة المخاطر التي تتعرض لها خلال مزاولة أنشطتها، كما تتضمن الإفصاح والشفافية اللازمين

بين هذه الشركات وجميع أصحاب المصلحة. تُعد الإدارة السليمة للمخاطر عنصراً أساسياً في قطاع التأمين في هذه المرحلة، نظراً لطبيعة هذا النشاط الذي يعتمد بشكل كبير على أساس من الثقة والشفافية لنمو الشركة واستقرارها. ولتحقيق أهداف هذه الدراسة، طرحنا مجموعة من الأسئلة على المدققين الداخليين في الهيئة، وجمعنا وحللنا مجموعة من الإجابات والمعلومات ذات الصلة بالدراسة الخاصة بالشركة. وخلصت الدراسة إلى عدة نقاط رئيسية، أهمها: - للتأمين أنواع مختلفة، تسعى جميعها إلى تقليل المخاطر التي قد تصيب الأشخاص أو الممتلكات من خلال شركات التأمين التي تدرس وتدير المخاطر المختلفة التي يتعرض لها المؤمن له. - يقوم التأمين على مبدأ تقاسم المخاطر، ويُحسب قسط التأمين بناءً على وظيفة المؤمن له أو مهنته، مما يضمن أن يكون القسط في متناوله. تُعتبر إدارة المخاطر وسيلةً فعالة لمواجهة المخاطر التي تتعرض لها شركة التأمين. وأهم المخاطر التي تواجه الشركة هو خطر الإفلاس، ومجلس الإدارة هو من يضع أساليب مواجهة المخاطر التي تواجه الشركة.

2. دراسة أيوب (2019) بعنوان: دور التدقيق الداخلي في إدارة مخاطر السيولة: دراسة ميدانية

لمجموعة بنوك "بنك الفلاحة والتنمية الريفية، بنك الجزائري الخارجي، بنك الخليج الجزائري"

ورقلة

تهدف هذه الدراسة إلى التعرف على التدقيق الداخلي ودوره في إدارة مخاطر السيولة في المؤسسة المالية (بنك الفلاحة والتنمية الريفية، بنك الجزائري الخارجي، بنك الخليج الجزائري)، قد استخدم المنهج الوصفي في إجراء الدراسة وقد أعد استبيان خصيصاً لهذا الغرض ومن تم توزيعها على مجتمع الدراسة البالغ عدد (30) فرداً بالبنوك السالفة الذكر في فترة امتدت من 02 ماي إلى 20 ماي 2019 م، وقد توصلت الدراسة إلى مجموعة من النتائج أهمها تمتع المدقق الداخلي بالاستقلالية الكافية لأداء مهامه، بالإضافة إلى وجود وعي لدى المدققين الداخليين بأهمية دورهم في إدارة مخاطر السيولة في البنوك وكذا تعاونهم الكبير مع الجهة المسؤولة عن تحديد المخاطر ويتمثل ذلك في تقديمهم للاستشارات والتوصيات بشأن إدارة المخاطر وكل ما يتعلق بذلك.

3. دراسة المري (2020) بعنوان: أثر إدارة المخاطر على الأداء الاستراتيجي: ذكاء الأعمال كمتغير

وسيط في البنوك التجارية العاملة في دولة الكويت

هدفت هذه الدراسة إلى التعرف على أثر إدارة المخاطر على الأداء الاستراتيجي مع استخدام ذكاء الأعمال كمتغير وسيط في البنوك التجارية العاملة في دولة الكويت. ولتحقيق أهداف الدراسة، صمم الباحث استبانة للدراسة لتوزيعها على أفراد العينة المسحوبة من مجتمع الدراسة، والتي تكونت من الموظفين العاملين في الإدارة العليا والوسطى في البنوك التجارية العاملة في دولة الكويت، والبالغ عددهم 6462 إداريًا. وكانت العينة المسحوبة عينة عشوائية طبقية مكونة من 363 موظفًا يعملون في الإدارة العليا والوسطى في البنوك التجارية العاملة في دولة الكويت. وقد تم توزيع الاستبانة على عينة الدراسة، وتم استرداد 270 استبانة صالحة للتحليل. وقد تم التوصل إلى عدة نتائج أهمها: يوجد تأثير ذو دلالة إحصائية لإدارة المخاطر بأبعادها (مخاطر الوثائق، ومخاطر السمعة التنظيمية، ومخاطر الموارد البشرية، ومخاطر الثقافة التنظيمية) على الأداء الاستراتيجي في البنوك التجارية العاملة في دولة الكويت. هناك أيضًا تأثير لإدارة المخاطر بأبعادها (مخاطر الوثائق، ومخاطر السمعة التنظيمية، ومخاطر الموارد البشرية، ومخاطر الثقافة التنظيمية) على ذكاء الأعمال في البنوك التجارية العاملة في دولة الكويت. كما يوجد تأثير لذكاء الأعمال على الأداء الاستراتيجي في البنوك التجارية العاملة في الكويت من خلال تفعيل ذكاء الأعمال كمتغير وسيط. ركزت أبرز التوصيات على ما يلي: ضرورة تحديث آليات إدارة المخاطر في البنوك من خلال تعيين أفراد محددين للحصول على أي بيانات للعملاء؛ الحفاظ على سمعة البنوك فيما يتعلق بإجراءات الأمن؛ تشجيع الموظفين على فصل العلاقات الشخصية عن إجراءات العمل؛ وتقليل دوران الموظفين في البنك. كما توصي الدراسة بضرورة ضمان تحديث شبكة الإنترنت في البنوك التجارية العاملة في الكويت. كما يجب على إدارة البنك التركيز على رفع مستوى الأداء الاستراتيجي من خلال التحسين المستمر للأداء المالي، بالإضافة إلى معالجة ملاحظات وشكاوى العملاء. يجب تمييز الخدمات المصرفية عن تلك التي تقدمها البنوك المنافسة، ويجب على إدارة البنك ضمان الاحتفاظ بالموظفين الأكفاء.

4. دراسة الحسني (2022) بعنوان: أثر التفكير الاستراتيجي في إدارة المخاطر: الدور المعدل للدعم

المنظمي في شركات المقاولات العمانية

هدفت الدراسة إلى قياس أثر التفكير الاستراتيجي بأبعاده (القصد الاستراتيجي، والرؤية النظامية، وصياغة الافتراضات، والتفكير في الوقت المناسب، واغتنام الفرص) على إدارة المخاطر بأبعادها (تحديد المخاطر، وتقييم المخاطر، والاستجابة للمخاطر، والسيطرة عليها) في شركات المقاولات العمانية. كما هدفت إلى توضيح الدور المعدل للدعم التنظيمي في تحسين أثر التفكير الاستراتيجي على إدارة المخاطر لهذه الشركات. تكون مجتمع الدراسة من (205) شركة تمثل شركات المقاولات العمانية. وتم الاعتماد على أسلوب المسح الشامل، حيث تم توزيع (205) استبانة، واسترجاع (149) استبانة صالحة للتحليل الإحصائي. واستخدمت الدراسة المنهج الوصفي الكمي، وتم استخدام مجموعة من الأساليب الإحصائية لتحليل بيانات الدراسة، من أهمها معامل الانحدار والانحدار الهرمي. وتوصلت الدراسة إلى عدة نتائج، من أهمها وجود أثر ذي دلالة إحصائية للتفكير الاستراتيجي على إدارة المخاطر في شركات المقاولات العمانية. أكدت الدراسة أيضًا دور الدعم التنظيمي في تعزيز أثر التفكير الاستراتيجي على إدارة المخاطر في الشركات العمانية. وكشفت عن مستويات مرتفعة لأبعاد التفكير الاستراتيجي، باستثناء صياغة الفرضيات، ومستويات مرتفعة لأبعاد إدارة المخاطر. كما جاءت أهمية الدعم التنظيمي متوسطة. وفي ضوء النتائج، اقترح الباحث مجموعة من التوصيات التي من شأنها مساعدة إدارة شركات المقاولات العمانية على رفع مستويات التفكير الاستراتيجي وإدارة المخاطر والدعم التنظيمي، وتحقيق التوازن بينهما. وأوصت بأن تعمل الشركات العمانية على تطوير قدرات المديرين على استشراف المستقبل، وتشجيعهم على إعداد السيناريوهات والافتراضات. كما أوصت باستخدام أنظمة متطورة لرصد المخاطر، والاهتمام بشكل أكبر بالاستراتيجيات البديلة لمواجهة المخاطر، وعدم الاعتماد على خطة محددة. كما أكدت على أهمية إنشاء نظام مكافآت يتناسب مع مساهمات الموظفين، ومعاملتهم بعدالة في توزيع إجراءات العمل، وتوزيع المكافآت بشكل عادل، مما يساهم في خلق رضا والتزام الموظفين وتحسين الأداء.

5. دراسة المصري (2019) بعنوان: إدارة مخاطر الأعمال وأثرها في الميزة التنافسية: دراسة تطبيقية

في بنك صفوة الإسلامي

هدفت هذه الدراسة إلى دراسة أثر عمليات إدارة مخاطر الأعمال المالية والمصرفية (كتعبير عن مخاطر الأعمال) على الميزة التنافسية في بنك صفوة الإسلامي. ولتحقيق هدف الدراسة، تم تطوير استبانة مكونة من (فقرة واحدة) واختبار صدقها وثباتها. يتكون مجتمع الدراسة من الإدارة العليا، وإدارة الموارد البشرية، والإدارة المالية، وإدارة الفروع، وإدارة المخاطر، وإدارة التسويق، بالإضافة إلى العاملين في فروع بنك صفوة الإسلامي. بلغ حجم مجتمع الدراسة 150 مديراً بمستويات إدارية مختلفة، وتم استرداد 143 استبانة صالحة للتحليل، بنسبة استجابة بلغت 95% من المجيبين الذين يمثلون وحدة التحليل المستهدفة. وتمت المعالجة الإحصائية لاستجابات المدراء باستخدام الحزمة الإحصائية للعلوم الاجتماعية (SPSS). توصلت الدراسة إلى النتائج التالية: يوجد تأثير ذو دلالة إحصائية لعمليات إدارة المخاطر على جودة الخدمة مع دلالة ($\alpha = 0.05$) وقيمة تباين نموذج الانحدار الخطي المتعدد $F = 40.620$ وقبول فكرة نموذج الانحدار الخطي المتعدد من حيث قيمة تحليل التباين للتحقق من صحة نموذج الانحدار الخطي المتعدد، بينما بلغت القوة التفسيرية للتغير في جودة الخدمات المصرفية $R^2 = 0.541$. يوجد تأثير ذو دلالة إحصائية لعمليات إدارة المخاطر على التمايز في التعامل مع العملاء، مع دلالة ($\alpha < 0.05$)، وقيمة تباين نموذج الانحدار الخطي المتعدد $F = 25.671$ وقبول فكرة نموذج الانحدار الخطي المتعدد، من حيث قيمة تحليل التباين للتحقق من صحة نموذج الانحدار الخطي المتعدد، بينما بلغت القوة التفسيرية للتغير في جودة الخدمات المصرفية $R^2 = 0.427$. يوجد تأثير ذو دلالة إحصائية لعمليات إدارة المخاطر على الابتكار في برامج تقديم الخدمات للعملاء، مع دلالة ($\alpha = 0.05$)، وقيمة تباين نموذج الانحدار الخطي المتعدد $F = 29.225$ ، ويتم قبول فكرة نموذج الانحدار الخطي المتعدد، من حيث قيمة تحليل التباين للتحقق من صحة نموذج الانحدار الخطي المتعدد، بينما بلغت القوة التفسيرية للتغير في جودة الخدمات المصرفية $R^2 = 0.459$. يوجد تأثير ذو دلالة إحصائية لعمليات إدارة المخاطر على توقيت تقديم الخدمات، مع دلالة ($\alpha = 0.05$)، وقيمة تباين نموذج الانحدار الخطي المتعدد $F = 32.025$ ، والقوة التفسيرية للتغير في جودة الخدمات المصرفية $R^2 = 0.459$. تم قبول نموذج الانحدار الخطي المتعدد بالاعتماد على تحليل التباين (ANOVA)

للتحقق من صحة نموذج الانحدار الخطي المتعدد، بينما بلغت القوة التفسيرية للتغير في جودة الخدمات المصرفية $R^2 = 0.481$. واقترحت الدراسة ضرورة تعميق الوعي المعرفي بعمليات إدارة المخاطر من خلال إعطاء الأولوية لعمليات تقييم المخاطر، ثم خيارات التعامل معها. كما اقترحت الدراسة تعزيز الميزة التنافسية من حيث الحفاظ على توقيت تقديم الخدمة، والاهتمام بأنواع الابتكار في تقديم الخدمات للعملاء (المالية، والمصرفية، والإلكترونية، والخدمية) بهدف بناء جسور التواصل معهم بأساليب ذكية وفعّالة.

6. دراسة ملوك (2019) بعنوان: دور شركات التأمين في إدارة المخاطر الصناعية: دراسة ميدانية

للشركة الجزائرية للتأمين وإعادة التأمين "La CAAR" وكالة غليزان - رقم 414

تهدف هذه الدراسة إلى إبراز دور وأهمية شركات التأمين وإعادة التأمين في إدارة جميع المخاطر، وخاصة المخاطر الصناعية. ويتحقق ذلك من خلال تطوير أنظمة لإدارتها وأساليب التعامل معها ومواجهتها من خلال التأمين أو تحويلها إلى إعادة التأمين. وقد تحقق ذلك من خلال تناول وسائل إدارة المخاطر المختلفة، باعتبارها الوظيفة التي تضمن بقاء واستمرارية شركات التأمين والمؤسسات الأخرى في ظل الظروف البيئية المتغيرة والمعقدة. ولتوضيح ذلك، اعتمدنا على استبيان، حيث وزعنا 60 استمارة على موظفي وكالة LA CAAR للتأمين وإعادة التأمين. وبعد جمع الاستثمارات الصالحة للدراسة، قمنا بتحليلها باستخدام برنامج التحليل الإحصائي SPSS 20. وخلصنا إلى أن وكالات التأمين وإعادة التأمين تلعب دوراً أساسياً في إدارة المخاطر الصناعية من خلال توفير أساليب وأنظمة لمواجهتها، بهدف ضمان البقاء والاستمرارية.

7. دراسة محمد (2020) بعنوان: إطار عمل لإدارة مخاطر مياه السدود: دراسة حالة النيل الشرقي

تهدف الدراسة إلى بناء إطار عمل لإدارة المخاطر المحتملة ووضع استراتيجيات واضحة للتعامل معها. ويتحقق ذلك من خلال تطوير نظام إلكتروني يساهم في إدخال البيانات وعرضها واستخراج التفاصيل والبيانات التاريخية لمساعدة متخذي القرار من جميع القطاعات (الحكومة والكهرباء والبيئة والمجتمع والجيولوجيا) على اتخاذ قرارات سليمة بناءً على بيانات واضحة ودقيقة. وقد تم استخدام المنهج

الوصفي العلمي لبناء الإطار من خلال تحليل مكوناته باستخدام لغة النمذجة الموحدة (UML) واستخدام لغات تصميم الويب (PHP-HTML-CSS) لبناء النظام وتنفيذه. ومن أهم نتائج الدراسة أن النظام الجديد ساعد في استخراج معلومات دقيقة تساعد في عملية اتخاذ القرار. وقدمت توصيات لاستكمال الإطار وتحسينه ودمجه مع عدد من الوزارات. ولعله في الحكومة الإلكترونية يكون لبنة لبناء أفكار أسى تساعد السودان على التقدم والتطور.

8. دراسة ونزار (2019) بعنوان: إدارة المخاطر في البنوك التجارية وفق ESG: حالة عينة من البنوك التجارية العاملة في الجزائر- حاسي مسعود

هدفت هذه الدراسة إلى دراسة العلاقة بين تبني معايير الحوكمة البيئية والاجتماعية والمؤسسية (ESG) في منح الائتمان وإدارة المخاطر في البنوك. وقد استندت الدراسة إلى استبيان تم توزيعه على الموظفين الرئيسيين في البنوك التجارية العاملة في حاسي مسعود بولاية ورقلة خلال الفترة 2018-2019. وخلصت الدراسة إلى وجود اتجاه نحو تبني معايير الحوكمة البيئية والاجتماعية والمؤسسية في الإدارة ومنح الائتمان من خلال بُعد معايير الحوكمة. وخلصت الدراسة إلى أن البنوك في عينة الدراسة تُركز على إدارة المخاطر من خلال المؤشرات الكمية والتقليدية، في حين أن المؤشرات غير الكمية لا تزال في مراحلها الأولى من التطوير. كما خلصنا إلى وجود علاقة ذات دلالة إحصائية بين نموذج معايير الحوكمة البيئية والاجتماعية والمؤسسية وإدارة المخاطر من خلال تأثير بُعد المعايير الاجتماعية على المتغير التابع "إدارة المخاطر" في البنوك قيد الدراسة. كما أشارت نتائج تحليل التباين أحادي الاتجاه إلى عدم وجود فروق ذات دلالة إحصائية في تطبيق إدارة المخاطر، في حين توجد فروق في تبني نموذج معايير الحوكمة البيئية والاجتماعية والمؤسسية بين البنوك التجارية قيد الدراسة.

9. دراسة أيوب (2019) بعنوان: دور التدقيق الداخلي في إدارة مخاطر السيولة: دراسة ميدانية لمجموعة بنوك "بنك الفلاحة والتنمية الريفية، بنك الجزائري الخارجي، بنك الخليج الجزائري" ورقلة

تهدف هذه الدراسة إلى التعرف على التدقيق الداخلي ودوره في إدارة مخاطر السيولة في المؤسسات المالية (بنك الزراعة والتنمية الريفية، البنك الجزائري الخارجي، بنك الجزائر والخليج). وقد استخدم المنهج

الوصفي في إجراء الدراسة، حيث تم إعداد استبيان خصيصاً لهذا الغرض ثم توزيعه على مجتمع الدراسة البالغ (30) فرداً في البنوك المذكورة خلال الفترة الممتدة من 2 مايو إلى 20 مايو 2019. وقد توصلت الدراسة إلى مجموعة من النتائج أهمها أن المدقق الداخلي يتمتع باستقلالية كافية لأداء مهامه، بالإضافة إلى وجود وعي لدى المدققين الداخليين بأهمية دورهم في إدارة مخاطر السيولة في البنوك، وكذلك تعاونهم الكبير مع الجهة المسؤولة عن تحديد المخاطر، والذي يتمثل في تقديمهم الاستشارات والتوصيات فيما يتعلق بإدارة المخاطر وكل ما يتعلق بها.

10. دراسة جلول (2019) بعنوان: إدارة المخاطر في شركات التأمين: دراسة حالة الشركة الوطنية

للتأمين SAA وكالة غليزان للفترة "2016-2014"

تهدف هذه الدراسة المتواضعة إلى تسليط الضوء على الأساليب المختلفة التي تتبعها شركات التأمين لإدارة المخاطر التي تتعرض لها خلال مزاولة أنشطتها، كما تتضمن الإفصاح والشفافية اللازمين بين هذه الشركات وجميع أصحاب المصلحة. تُعد الإدارة السليمة للمخاطر عنصراً أساسياً في قطاع التأمين في هذه المرحلة، نظراً لطبيعة هذا النشاط الذي يعتمد بشكل كبير على أساس من الثقة والشفافية لنمو الشركة واستقرارها. ولتحقيق أهداف هذه الدراسة، طرحنا مجموعة من الأسئلة على المدققين الداخليين في الهيئة، وجمعنا وحللنا مجموعة من الإجابات والمعلومات ذات الصلة بالدراسة الخاصة بالشركة. وخلصت الدراسة إلى عدة نقاط رئيسية، أهمها: - للتأمين أنواع مختلفة، تسعى جميعها إلى تقليل المخاطر التي قد تصيب الأشخاص أو الممتلكات من خلال شركات التأمين التي تدرس وتدير المخاطر المختلفة التي يتعرض لها المؤمن له. - يقوم التأمين على مبدأ تقاسم المخاطر، ويُحسب قسط التأمين بناءً على وظيفة المؤمن له أو مهنته، مما يضمن أن يكون القسط في متناوله. تُعتبر إدارة المخاطر وسيلة فعالة لمواجهة المخاطر التي تتعرض لها شركة التأمين. وأهم المخاطر التي تواجه الشركة هو خطر الإفلاس، ومجلس الإدارة هو من يضع أساليب مواجهة المخاطر التي تواجه الشركة.

8.1 الفجوة البحثية

بناءً على مراجعة الدراسات السابقة المتعلقة بإدارة المخاطر، يُمكن تحديد الفجوة البحثية التي تسعى الدراسة الحالية إلى معالجتها من خلال تحليل محاور التركيز والاختلافات بين ما تناولته تلك

الدراسات وما تسعى هذه الدراسة إلى تسليط الضوء عليه من خلال تسليط الضوء على تأثير إدارة مخاطر العامل البشري في الحد من الهجمات الإلكترونية، وتحديدًا في بيئة المؤسسات الحكومية بالمملكة العربية السعودية.

تناولت دراسة الحلول لعام 2019 إدارة المخاطر في قطاع التأمين من منظور تقليدي، مُركزةً على المخاطر المالية والتشغيلية، مع التركيز على الكيانات المؤسسية ككل، دون التطرق إلى العامل البشري بشكل منفصل أو التهديدات الرقمية المرتبطة به. علاوةً على ذلك، ركزت الدراسة على مؤسسة واحدة في سياق جزائري محلي، ولم تتعمق في العلاقة بين سلوك الأفراد داخل المؤسسة وقابليتها للتأثر بالمخاطر غير التقليدية كالهجمات الإلكترونية. وهذا يُبعدنا عن السياق الإلكتروني المُعقد الذي تناوله الدراسة الحالية، والذي يضع العامل البشري في قلب منظومة التهديدات المعلوماتية ويُحلل تأثيره من منظور أمني.

ركزت دراسة أيوب (2019) على دور التدقيق الداخلي في إدارة مخاطر السيولة في القطاع المصرفي. يُعد هذا الأمر مهمًا في السياق المالي، إلا أنه يتناول نوعًا محددًا من المخاطر (السيولة) ويرتبط بوظيفة محددة (التدقيق الداخلي). كما ركزت الدراسة على تقييم استقلالية المدققين الداخليين وقدرتهم على تقديم توصيات فعّالة للحد من المخاطر المالية، دون التطرق إلى المخاطر البشرية ذات الطابع الأمني أو التقني، كالهجمات الإلكترونية الناتجة عن الإهمال أو الجهل بالإجراءات أو التفاعل اللاواعي مع محاولات الاختراق. لذا، تفتقر هذه الدراسة إلى دراسة ممارسات إدارة المخاطر المتعلقة بالعامل البشري في البيئات الرقمية، مما يُبرر ضرورة تسليط الدراسة الحالية الضوء على هذا الجانب المُغفل.

من ناحية أخرى، تُعتبر دراسة المري (2020) دراسة متقدمة نسبيًا، حيث تناولت تأثير إدارة المخاطر على الأداء الاستراتيجي، بما في ذلك "ذكاء الأعمال" كمتغير وسيط. وقد قدمت رؤية شاملة لأبعاد المخاطر في بيئة العمل المصرفي التجاري في دولة الكويت. مع ذلك، وبينما تناولت هذه الدراسة بعض جوانب المخاطر المتعلقة بالموارد البشرية والثقافة التنظيمية، إلا أنها لم تُركز بشكل مباشر أو مُفصّل على العلاقة بين المخاطر السلوكية للعامل البشري والتهديدات السيبرانية التي قد تنتج عنها. كما لم تُعالج التحديات الرقمية أو الأمن السيبراني كخطر ناشئ. علاوةً على ذلك، أُجريت الدراسة في سياق مصرفي تجاري، يختلف

بطبيعته عن بيئة المؤسسات الحكومية، باختلاف هياكلها الإدارية والتنظيمية، وتزايد اعتمادها على التحول الرقمي والتقنيات الحساسة في المملكة العربية السعودية.

في ضوء ما سبق، يتضح أن جميع الدراسات السابقة ركزت على المخاطر المؤسسية والمالية والإدارية التقليدية، دون التطرق إلى البعد السيبراني المتعلق بالعامل البشري، على الرغم من الأهمية المتزايدة لهذا الموضوع عالميًا ومحليًا. علاوة على ذلك، اقتصر السياق المكاني لهذه الدراسات على دول عربية كالكويت والجزائر، دون تغطية البيئة السعودية التي تتميز بتحول رقمي واسع ضمن رؤية المملكة 2030. وهذا يُضاعف من أهمية دراسة التهديدات السيبرانية المتعلقة بالعامل البشري في القطاع الحكومي.

وبناءً على ذلك، تُسدّ الدراسة الحالية ثغرةً بحثيةً واضحةً من خلال تسليط الضوء على إدارة مخاطر العامل البشري كنهجٍ رئيسيٍّ للحدّ من الهجمات السيبرانية. يجمع هذا الموضوع بين الأبعاد الإدارية والسلوكية والتقنية، ولم تُعالج الدراسات السابقة بشكلٍ مباشرٍ وشامل، لا من حيث المحتوى ولا من حيث السياق العملي. كما تسعى الدراسة إلى تقديم رؤيةٍ ميدانيةٍ واضحةٍ مبنيةٍ على بياناتٍ واقعيةٍ من المؤسسات الحكومية السعودية، مما يُضفي على نتائجها قيمةً علميةً وعمليةً يُمكن توظيفها لتحسين ممارسات الأمن السيبراني في المملكة.

في دراسة الحسني (2022)، ركزت الدراسة على العلاقة بين التفكير الاستراتيجي وإدارة المخاطر في شركات المقاولات العمانية، من خلال تحليل الأثر المباشر للدعم التنظيمي في تحسين العلاقة بين المتغيرين. ورغم أهمية هذه الدراسة في تسليط الضوء على الأبعاد الذهنية والاستراتيجية لإدارة المخاطر، إلا أنها لم تتطرق إلى طبيعة المخاطر المرتبطة بالعامل البشري، وخاصةً تلك المتعلقة بالسلوكيات الفردية التي قد تُسبب ثغرات في الأمن السيبراني، وهو محورٌ أساسيٌّ للدراسة الحالية. ويُبرز غياب البعد التقني أو الرقمي في دراسة الحسني الحاجة إلى بحوث تُدمج السلوك البشري مع تقنيات الأمن الحديثة.

9.1 المنطلقات النظرية للدراسة

تنبع هذه الدراسة من حاجة ملحة فرضها التوسع الهائل في البيئة الرقمية المعاصرة. فقد أصبحت الهجمات الإلكترونية من أخطر التهديدات التي تواجه المؤسسات بمختلف أنواعها، لا سيما مع تزايد

الاعتماد على التكنولوجيا في معالجة المعاملات وتخزين البيانات وتشغيل العمليات. وفي ظل هذا التحول، بات من المسلّم به أن الأمن السيبراني يتجاوز الحماية التقنية، ليشمل سلوك الأفراد داخل المؤسسة. وقد أثبتت الدراسات والتقارير العالمية أن نسبة كبيرة من الاختراقات ناتجة عن خطأ بشري أو سلوك غير آمن، مثل فتح روابط ضارة، أو تسريب بيانات حساسة، أو استخدام كلمات مرور ضعيفة. وقد أدى ذلك إلى وصف "العامل البشري" بأنه "الحلقة الأضعف" في نظام الأمن الرقمي.

وبناءً على ذلك، تستند الدراسة الحالية إلى إطار نظري أساسي قائم على نظرية النظم، والذي ينظر إلى المؤسسة كنظام مترابط يتكون من وحدات فرعية (بشرية، وتقنية، وتنظيمية) تتفاعل مع بعضها البعض وتتأثر بمحيطها. وفقًا لهذه النظرية، فإن أي ضعف أو خلل في أحد مكونات النظام - كالعامل البشري - قد يؤدي إلى خلل في أداء النظام بأكمله. وينطبق هذا بوضوح على الأنظمة الرقمية التي تعتمد على تفاعل المستخدم مع الموارد التكنولوجية. ومن هذا المنظور، فإن إدارة مخاطر العامل البشري ليست عنصرًا ثانويًا، بل هي عنصر أساسي لضمان استقرار وفعالية النظام السيبراني.

وتستند الدراسة أيضًا إلى مفاهيم إدارة مخاطر المؤسسات (ERM)، التي تفترض أن كل مؤسسة تعمل في بيئة معقدة ومحفوفة بالمخاطر، وبالتالي فهي مطالبة بوضع سياسات وإجراءات لتحديد هذه المخاطر وتحليلها ومعالجتها وفقًا لأولوياتها. وفي هذا السياق، يُعامل العامل البشري هنا كمصدر للخطر - ليس بالضرورة بسبب نية الإضرار، بل بسبب احتمالية السلوك غير الآمن نتيجة ضعف الوعي أو نقص التدريب أو نقص الرقابة. وتُعد القدرة على التنبؤ بهذه السلوكيات وتطوير آليات للتخفيف منها جزءًا لا يتجزأ من نظام الحماية الاستباقي.

تعتمد هذه الدراسة أيضًا على مبادئ نظرية السلوك التنظيمي، التي تُركز على فهم سلوك الأفراد في مكان العمل والعوامل المؤثرة في قراراتهم وأفعالهم. ووفقًا لهذا الإطار، فإن بناء ثقافة أمنية تنظيمية، وغرس الوعي السيبراني، وتوفير الحوافز المناسبة، ومراقبة الأداء، كلها وسائل فعّالة لإدارة المخاطر البشرية، وبالتالي الحد من التهديدات التي قد تنشأ. قد لا يكون السلوك غير الآمن نتيجةً للجهل فحسب، بل قد ينتج أيضًا عن ضغوط العمل، وضعف الالتزام التنظيمي، أو غياب ثقافة المساءلة.

في هذا السياق، تكتسب هذه الدراسة أهميتها من محاولتها الجمع بين الأطر النظرية الثلاثة: المخاطر النظامية، والسلوكية، والمؤسسية، لتفسير ظاهرة لم تحظَ باهتمام كافٍ في الأدبيات، وخاصةً في البيئات الحكومية العربية. مع تزايد تعرض المؤسسات الحكومية للهجمات السيبرانية، وخاصةً في ظل التحول الرقمي الشامل في المملكة العربية السعودية، تبرز الحاجة إلى نماذج تحليلية تربط مباشرةً بين السلوك البشري وأمن المعلومات، وتقدم حلولاً عملية قائمة على أسس علمية واضحة.

بناءً على هذه الفرضيات النظرية، تفترض الدراسة أن إدارة مخاطر العامل البشري - من خلال التوعية والتدريب والرصد والتحفيز - تُعدّ نهجاً فعالاً ومتكاملاً للحد من الهجمات السيبرانية، وتُسهم بشكل مباشر في رفع مستوى المرونة الرقمية للمنظمات. لذا، تسعى الدراسة إلى توفير إطار عمل تطبيقي قائم على أسس علمية، يُمكن من خلاله قياس فعالية هذه الإدارة وأثرها في بيئة رقمية متنامية، بما يلبي متطلبات الأمن السيبراني للقطاع الحكومي في المملكة.

10.1 المنهجية وطرق البحث:

تم اتباع المنهج الوصفي والمنهج التحليلي كأسلوب مناسب للوصف، الذي يتطابق مع الفصول النظرية أما في الفصل التطبيقي التحليلي والمنهج الاستنباطي من أجل تحليل وتقييم البيانات المتحصل عليها في الاستبانة للمؤسسة محل الدراسة باعتباره ملائماً لتقرير الحقائق وفهم مكونات الموضوع، مع إخضاعه للدراسة الدقيقة وتحليل أبعاده، والتي سنتطرق إليها في الفصل التطبيقي في دراسة الحالة.

يعتمد اختيار المنهج الملائم لطبيعة البحث على طبيعة المشكلة والهدف من دراستها، ومن أجل الإحاطة بمختلف جوانب الدراسة سيتم الاعتماد على المنهج الوصفي التحليلي، فالأسلوب الوصفي مناسب للوصف الذي يتطابق مع الفصول النظرية، أما في الفصل التطبيقي التحليلي والمنهج الاستنباطي من أجل تحليل وتقييم البيانات المتحصل عليها في الاستبانة محل الدراسة، حيث يسهم هذا المنهج في الإجابة عن التساؤلات البحثية من خلال جمع البيانات ومن ثم تحليلها ومناقشتها. وهذا المنهج هو المستخدم في معظم الدراسات السابقة.

11.1 مصادر جمع البيانات

- المصادر الثانوية: وتشمل البيانات والمعلومات الموجودة في الكتب والمراجع، والرسائل الجامعية وأوراق العمل والمجلات والدوريات والمؤتمرات العلمية وورش العمل، بالإضافة إلى التقارير المنشورة وغير المنشورة التي تناولت الموضوع في مختلف المؤسسات ذات الصلة.
- المصادر الأولية: اعتمدت الدراسة على الاستبانة كأداة رئيسية في جمع البيانات من مصادرها والتي تم تصميمها خصيصاً لهذا الغرض على Google Forms وإرسال رابطها إلى مجتمع البحث.

12.1 أدوات الدراسة:

- تعرف أداة البحث بأنها "الوسيلة التي تتم بواسطتها عملية جمع البيانات بهدف الإجابة عن تساؤلاته، وسيعتمد الباحثين في جمع البيانات على الاستبانة، والتي تُعرف بأنها "صيغة محددة من الفقرات والأسئلة تهدف إلى جمع البيانات من أفراد البحث"
- حيث تكونت من قسمين رئيسيين هما:

- القسم الأول: وهو الجزء الخاص بالمتغيرات الديمغرافية لأفراد عينة الدراسة، والمتمثلة بـ: النوع، والعمر، والمؤهل العلمي، والمستوى الوظيفي.
- القسم الثاني: اشتمل القسم الثاني على الفقرات والأبعاد التي تقيس متغيرات الدراسة المستقل والتابع.

13.1 الأساليب الإحصائية المستخدمة

تم استخدام الأساليب الإحصائية التالية لتحقيق أهداف الدراسة:

- معامل " ألفا كرونباخ " لقياس ثبات أداة الدراسة ومعامل الارتباط بيرسون لقياس صدق أداة الدراسة والعلاقة بين المتغيرات

- التكرارات والنسب المئوية والمتوسط الحسابي والانحراف المعياري المتعلقة بمتغيرات الدراسة ولجميع الاستجابات على فقرات الاستبيان.
- معامل الانحدار الخطي البسيط لقياس أثر كل بعد من أبعاد المتغير المستقل على المتغير التابع

14.1 أداة الدراسة

تم تصميم الاستبانة في الدراسة الحالية لتتناسب مع متغيرات البحث من خلال الاطلاع على الدراسات السابقة ذات الصلة بموضوع الدراسة. تتكون الاستبانة من قسمين رئيسيين:

- ✓ **القسم الأول:** يتناول المتغيرات الديمغرافية لأفراد عينة الدراسة من العاملين في وزارة الصحة السعودية، ويشمل المسمى الوظيفي، العمر، المستوى التعليمي، وعدد سنوات الخبرة.
- ✓ **القسم الثاني:** يحتوي على الفقرات التي تقيس المتغيرات المستقلة والتابعة في الدراسة.

أولاً: المتغير المستقل – إدارة مخاطر العامل البشري، ويُقاس من خلال 15 فقرة مقسمة أربعة أبعاد رئيسية:

1. المعرفة التقنية
2. تشخيص الأعطال
3. تطوير القدرات الذاتية
4. الالتزام بمعايير السلامة

ثانياً: المتغير التابع – الهجمات السيبرانية، ويُقاس من خلال (10) فقرة موزعة.

15.1 حدود الدراسة:

- ✓ **حدود مكانية:** تُجرى الدراسة على المؤسسات الحكومية في المملكة العربية السعودية

✓ **حدود موضوعية :** تقتصر الدراسة على تحليل أثر تطبيق إدارة مخاطر العامل البشري بأبعادها

مجموعة المتمثلة في (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد

من الهجمات السيبرانية

✓ **حدود زمانية :** تم إعداد الدراسة في عام 2025.

✓ **حدود بشرية:** تقتصر الحدود البشرية لهذه الدراسة على العاملين في المؤسسات الحكومية في المملكة

العربية السعودية، ممن لديهم ارتباط مباشر بالأعمال الحكومية

الفصل الثاني: الإطار النظري

المبحث الأول: فهم العوامل البشرية وتشريح الأخطاء النظامية

1.1.2 المقدمة

تُعدّ إدارة مخاطر العامل البشري من أكثر التحديات تعقيداً في منظومة الحوكمة المؤسسية، إذ تتشابك فيها عناصر السلوك الفردي، والثقافة التنظيمية، وسياسات الموارد البشرية، والضغوط البيئية والتقنية المحيطة بالموظف. تبدأ هذه الإدارة بفهم معمّق لماهية "العامل البشري" بوصفه مجموعة من القدرات والحدود النفسية والمعرفية والجسدية التي تؤثر في الأداء اليومي للأفراد. فالأخطاء الناجمة عن الإرهاق أو التوتر أو ضعف التدريب ليست حوادث معزولة، بل أعراض لنظام عمل قد يفتقر إلى التوازن بين متطلبات الإنتاج واحتياجات الإنسان. من هنا يأتي دور الإدارة في تحليل السياق الداخلي والخارجي لاكتشاف نقاط الضعف السلوكية المتكررة، مثل الاعتماد المفرط على الذاكرة، أو مقاومة التغيير، أو الثقة الزائدة في أنظمة الأتمتة، ثم تحويل هذه الاكتشافات إلى فرضيات قابلة للقياس والمتابعة. (Al-Salahi & Al-Tarawneh, 2024)

يمتد نطاق إدارة مخاطر العامل البشري إلى تصميم عمليات استقطاب وتوظيف تضع كفاءة المرشح على صعيد السلامة والسلوك الأخلاقي في مرتبة لا تقل أهمية عن الكفاءة الفنية. فالمقابلات المبنية على الكفايات، والتقييمات النفسية، واختبارات تحمّل الضغط، ليست أدوات انتقائية فحسب، بل خطوط دفاع استباقية تقلص احتمال ظهور سلوكيات قد تُفضي إلى خسائر مالية أو سمعة سلبية. وبعد الاستقطاب تبرز أهمية التهيئة الوظيفية الممنهجة التي توضح للموظف الجديد طبيعة المخاطر المرتبطة بدوره، وتحفّزه على تبني عقلية تقدّر الإبلاغ المبكر عن المشكلات. (Al-Dhawadi, 2020)

2.1.2 الهندسة البشرية وتصميم بيئة العمل الآمنة

يلعب تصميم بيئة العمل دوراً محورياً في خفض احتمالية الخطأ البشري؛ فالإضاءة السيئة أو الضوضاء أو واجهات الاستخدام المعقّدة ترفع مستويات التشتت وتزيد من زمن التفاعل مع المهام

الحساسية. تعتمد المؤسسات الرائدة مبادئ الهندسة البشرية لإعادة تشكيل أماكن العمل بحيث تُوضَع الأدوات الحرجة في محيط إدراكي واضح، وتُزوّد أجهزة التحكم بتنبيهات بصرية وصوتية تمنع التشويش وتسهّل اتخاذ القرار. كما تُستخدم المحاكاة والواقع الافتراضي لتدريب الموظفين على سيناريوهات عالية الخطورة حتى يتحوّل الرد السليم إلى عادة راسخة . (Ramadan, 2022)

لا يمكن فصل إدارة مخاطر العامل البشري عن ثقافة المؤسسة في ما يتعلق بالشفافية والإفصاح. فنهج "الثقافة العادلة" يميّز بين الأخطاء غير المقصودة والسلوك المتعمّد المخالف، ويشجع الموظفين على الاعتراف بالهفوات فور وقوعها. يعتمد نجاح هذا النهج على دعم الإدارة العليا وترسيخ قيم تؤكد أن الهدف هو تحسين النظام لا البحث عن كبش فداء، لتتحول التحقيقات من محاسبة إلى أداة تعلّم تنظيمي مستمر . (Abdul Jader, 2022)

تتطلّب الرقابة الفعّالة على المخاطر البشرية بنية تقنية متقدمة تجمع بين أدوات القياس اللحظي للأداء وأدوات التحليل التنبئي. فأنظمة مراقبة الإجهاد القابلة للارتداء تقدّم قراءات حية لمستويات الإرهاق وتربطها بمنصات ذكاء اصطناعي تستشرف متى ترتفع احتمالية الخطأ الحرج. غير أن الاعتماد على التكنولوجيا لا يُغني عن دور القيادة؛ فالتواصل المباشر، والدعم النفسي، وبرامج التوازن بين الحياة والعمل تظل مقومات لا يمكن للأتمتة أن تعوّضها . (Awad & Al-Khazaali, 2022)

تُختتم دورة إدارة مخاطر العامل البشري بعملية مراجعة شاملة تستلهم مبادئ التحسين المستمر. تُقاس فجوات الأداء بمؤشرات كمية مثل عدد الحوادث وشدّتها، وبمقاييس نوعية كرضا الموظفين وثقتهم بالنظام. تُستخدم النتائج لتحديث سياسات التوظيف والتدريب والتقنية، فيتحول الجانب البشري من عامل تهديد إلى مصدر أفضلية تنافسية يرفع موثوقية العمليات ويعزّز سمعة المؤسسة . (Attia, Obaidat & Al-Saghir, 2024)

تؤطّر المنظمات المتقدمة إدارة مخاطر العامل البشري ضمن منظومة تشريعية ومعيارية تضمن التوافق مع القوانين المحلية والاتفاقيات الدولية. فالقطاعات عالية الحساسية تستند إلى معيار ISO 45001 ومنهجيات Crew Resource Management لضبط التعاون واتخاذ القرار تحت الضغط. تُتيح هذه

الأطر لغة مشتركة لتصنيف المخاطر وتصميم ضوابط وقائية وعلاجية عابرة للحدود، وتؤسس لدورة تدقيق وتحسين تُبقي سياسات المخاطر البشرية حيّة لا موسمية . (Al-Tarawneh, Al-Jubouri & Al- Maaytah, 2020)

3.1.2 إدماج المخاطر البشرية في منظومة إدارة المخاطر المؤسسية

لكي تتكامل المخاطر البشرية مع إدارة المخاطر المؤسسية (ERM) ، يجب ربط تحليلات الأداء البشري بمصفوفة المخاطر الشاملة بحيث يظهر أثر السلوك الفردي في الربحية والامتثال والاستعداد للأزمات. يؤدي إشراك خبراء العوامل البشرية في لجان المخاطر إلى كشف "الذخيرة المعرفية" الحرجة التي قد تتآكل بمرور الوقت، فيغدو الإنسان بوابة لمخاطر وفرص معقدة على حدّ سواء . (Debbache, Roula & Benfenatki, 2023)

يكتسب القياس هنا بعداً علمياً عبر مؤشرات أداء (KPIs) ومؤشرات مخاطر (KRIs) مصمّمة خصيصاً للبُعد البشري. تُحلّل بيانات مثل زمن الاستجابة للإنذارات ونسبة الأخطاء المُصحّحة ذاتياً ومعدل تبني الإجراءات الجديدة. وتذهب بعض المؤسسات أبعد من ذلك فتستخدم خوارزميات معالجة اللغة الطبيعية لمسح البريد الداخلي ومنصات التواصل المهني لرصد أنماط الانفعال أو تدني الروح المعنوية قبل أن تتحول إلى حوادث. ينشأ بذلك "مخطط حرارة" بشري لحظي يوفّر رؤية استباقية، مع مراعاة سياسات خصوصية شفافة تجعل العملية شراكة لا مراقبة قسرية . (Hamed, 2023)

يظل التغيير التنظيمي، ولا سيما التحول الرقمي، أحد أكبر مولّدات المخاطر البشرية. فالانتقال من أنظمة تقليدية إلى حلول ذكاء اصطناعي قد يخلق فجوة مهارية وقلقاً مهنيّاً يخفض التركيز والالتزام. تتعامل المؤسسات الرصينة مع ذلك عبر برامج تغيير تدريجيّ تمزج التدريب العملي بمشاركة الموظفين في تصميم العمليات الجديدة، وتراقب مؤشرات مثل معدل الأخطاء بعد النشر ومستوى اللجوء إلى قنوات الدعم لتصحيح المسار سريعاً . (Maqbul, 2024)

مع تبني نماذج العمل عن بُعد وسلاسل التوريد العالمية، يطفو البُعد الثقافي والاختلاف القانوني على السطح كعوامل تضاعف مخاطر العامل البشري. فالموظف الذي يعمل من منطقة زمنية مختلفة قد

يواجه ضغطاً خفياً للاستجابة خارج ساعات العمل، ما يرفع احتمال الإرهاق. وللمحد من ذلك تعتمد بعض الشركات بروتوكولات "فصل رقمي" ملزمة وخوارزميات جدولة تُوازن عبء العمل بين الأقاليم، فيما تفرض على المتعاقدين مدونات سلوك موحدة وآليات تدقيق عابرة للحدود . (Al-Ramadan et al., 2022)

4.1.2 التنوع والشمولية كصمام أمان سلوكي

تشير الأبحاث إلى أن فرق العمل المتنوعة أكثر قدرة على كشف الأخطاء وتحدي الافتراضات من الفرق المتجانسة. لكن تحويل التنوع إلى خط دفاع فعلي يتطلب بيئة "أمان نفسي" تسمح بالتعبير عن المخاوف بلا خوف من الانتقام. مبادرات الرفاه والدعم السلوكي وسياسات الإجازات المرنة تقلص خطر الإرهاق والتوتر المزمن، وترفع في الوقت نفسه جاذبية المؤسسة للمواهب رفيعة الكفاءة . (Al-Balawi, 2025)

عند وقوع حادث أو نشوب أزمة واسعة النطاق، يظهر أثر إدارة مخاطر العامل البشري في سرعة الاستجابة والتعافي. فالخطط المكتوبة تتحول إلى واقع إذا دُعمت بتدريب يحاكي الانقطاعات الحقيقية ويُعرّف الأدوار بوضوح ويمنح الموظفين سلطة اتخاذ القرار عند غياب القيادات العليا. المؤسسات التي خصصت "سفراء مرونة" داخل كل وحدة عمل استعادت عملياتها بكلفة أقل من تلك التي راهنت على الحلول التقنية وحدها، ما يؤكد أن الفرد يظل نقطة الارتكاز التي تصل بين الخيوط المادية والرقمية وتحول الإجراءات إلى أداء فعلي يحمي الأرواح والأصول معاً . (Dohi, 2024)

5.1.2 هندسة "النقطة الحمراء" واستباق الخطأ السري

في بيئات الرعاية الصحية عالية الضغط ظهر مفهوم "النقطة الحمراء" ليصف اللحظة الدقيقة التي يبتعد فيها القرار الطبي عن المسار الآمن من دون أن ينتبه أحد. تُشرح دراسات معهد جونز هوبكنز أن هذه اللحظة تستغرق في المتوسط 17 ثانية من التردد الصامت قبل إعطاء جرعة دواء أو تأكيد تشخيص. ولمنع الانجراف، طُوّر بروتوكول يسجل خلاله طبيبُ الامتياز فيديو قصيراً لا يتجاوز ثلاثين ثانية يصف فيه الحالة ونية الإجراء ويرفعه إلى استشاري مناوب عبر منصة مشفرة. إذا لم يضغط الاستشاري زرّ "إقرار"

خلال ثلاث دقائق يتحول الخط إلى اللون الأحمر على لوحة مركزية في غرفة العمليات فيتدخل فريق سلامة مستقل. بعد عام واحد من التطبيق انخفضت الأخطاء الدوائية الجسيمة 28 %، ما يؤكد أن تحويل اللحظات الغامضة إلى مؤشرات بصرية صارمة يكسر تسلسل الخطأ قبل اكتماله. (Abu Alead & Ab (Altalibe, 2023

تكشف أبحاث جامعة إموري أن الموظف لا يبلغ عن الخطأ إلا إذا تأكد أن إجراءات التحقيق ستطبق عليه وعلى زملائه بمعيار واحد. لذلك تبنت شركة طيران آسيوية "مصفوفة العدالة الإجرائية" التي تلزم المحقق بإعلان سبب اختيار كل شاهد أو وثيقة قبل بدء التحقيق، ويُنّاح للموظف المشتبه بخطئه اقتراح مصادر بيانات إضافية للدفاع عن نفسه. نُشرت هذه المصفوفة على لوحة رقمية مفتوحة لكل العاملين، فارتفع مؤشر الإبلاغ الطوعي 46 % خلال ستة أشهر لأن الثقة في عدالة المسار حدثت من الخوف الذي كان يكتم الحوادث الصغيرة ويحوّلها إلى كوارث لاحقاً. (Al-Muadat, Bani Ahmed & Al-Durgham, 2023

عندما يُكرّر الموظف المهمة نفسها آلاف المرات تتراجع مستوياته الإدراكية بسبب ظاهرة " الانطفاء المهاري"؛ إذ يستعيز الدماغ عن التفكير النشط بسلسلة أوامر أوتوماتيكية قد لا تعالج الحالات الشاذة. رصدت مصانع أشباه الموصلات اليابانية هذه الظاهرة عبر تحليل زمن التوقف الذهني بين الضغوطات على لوحة التحكم فوجدت أن الانطفاء يبدأ بعد ثمانية أسابيع من مناوبات متماثلة. ولعكس الاتجاه، أدخلت الشركة "بروتوكول القلب النابض" الذي يجبر النظام على تغيير ترتيب خطوات الضبط مرة كل عشر عمليات، فيُضطر العامل إلى استدعاء ذاكرته الإجرائية والتأكد يدوياً من كل متغير بدلاً من الانسياق وراء العادة. النتيجة: انخفاض أخطاء الضبط الدقيقة 19 % وارتفاع الاستبقاء الوظيفي لأن الملل المزمن تراجع بدوره. (Al-Tamimi & Mughaid, 2024)

6.1.2 الذكاء الثقافي وإدارة مخاطر القوى العاملة متعددة الجنسيات

توظّف الشركات العابرة للقارات آلاف العاملين من ثقافات متباينة، ولكل ثقافة مدونة صامتة لما يُعتبر خطأ أو مخالفة. فالفني الإسكندنافي قد يوقف الآلة فوراً عند سماع صوت غير مألوف، بينما زميله

من جنوب شرق آسيا يتردد احتراماً للتسلسل الهرمي. أنشأت شركة طاقة بريطانية قاعدة بيانات "مواقف ثقافية حرجة" تُوقّر سيناريوهات واقعية تشرح ما يراه كل شعب واجباً وما يراه خروجاً على النظام. تُستخدم هذه القاعدة في برنامج واقع افتراضي يضع الفريق متعدد الجنسيات في غرفة تحكّم مشتركة تحاكي حادث تسرب غاز. بعد ثلاث جولات تدريبية تحسّن زمن اتخاذ القرار الجماعي 35 %، ما يبرهن أن رفع معامل الذكاء الثقافي يخفّض أثر الصمت أو المجاملة المفرطين باعتبارهما أخطاء بشرية مقنّعة. (AI-) (Quraan & Obaidat, 2023)

يعود مصطلح "منحنى كوبرا" إلى قصة استعانت فيها حكومة استعمارية بمكافآت مالية لقتل الأفاعي، فبدأ الناس يربّونها سرّاً للحصول على الجائزة. في المؤسسات المالية يظهر المنحنى عندما تُربط مكافآت السماسرة بعدد الصفقات لا جودتها؛ فيتضاعف حجم الأخطاء التداولية بسبب التسرّع. اعتمد بنك استثماري أوروبي "مقياس صافي القيمة الآمنة" الذي يخصم من المكافأة نقاطاً تساوي المخاطر التي تعرّض لها رأس المال فوراً، بدلاً من انتظار نهاية السنة المالية. ترافق هذا مع جلسات تحليل نفسي تشرح للسّمسار انعكاس إفراط الأدريينالين على كفاءة القرار. بعد عامين انخفض تكرار تجاوز حدود الانتمان الفوري بنسبة 60 % وتساوى متوسط الدخل المسجّل مع سنوات الازدهار ولكن بمخاطر أقل مرتين. (Albalushi, Ali & Aman, 2022)

تزداد أهمية فهم "بصمة السلوك" لدى العاملين في المواقع الحرجة كلما ارتفعت سرعة الإنتاج واشتدت ضغوط التسليم. تعتمد الهندسة السلوكية على تفكيك مهام الفرد خطوة بخطوة، وتحديد متى تقتضي الدقة القصوى أو التركيز الإدراكي العالي، ومتى يمكن الاستعانة بالذاكرة الإجرائية أو الأتمتة الجزئية. تنفذ بعض شركات تصنيع السيارات دراسات "عيون الكاميرا" حيث تُسجّل نظرة العامل ومسار يده بدقة عالية أثناء إجراء معقّد مثل تركيب وحدة الأمان في الوسادة الهوائية. بمجرد اكتشاف نقاط الانحراف، يعاد تصميم محطة العمل بتقليل تشويش الحواس وإضافة عناصر إشعار لوني يذكّر العامل بخطوات قد يفوتها بسبب الإرهاق. ونتيجة لذلك انخفض زمن التشغيل غير المطابق لتحملات الجودة بنسبة 15 % في سنة واحدة، كما تحسّنت مؤشرات رضا الموظفين لتراجع الضغط الذهني السلبي. (Ahmed, Kazar & Harous, 2024)

رغم وفرة أدوات الرقابة التقنية، تظل المتابعة الذاتية ركيزة أساسية في إدارة مخاطر العامل البشري. طوّرت مؤسسات الطيران نظام "التصريح الطوعي بالضغوط" الذي يُطلب فيه من الطيار أو المراقب الجوي تعبئة تقرير قصير حول مستوى توتره أو جودة نومه قبل المناوبة. تُخزّن هذه البيانات في قاعدة آمنة، ويُنبه الخادم المركزي عند ارتفاع مؤشر الإرهاق الفردي فوق عتبة معينة لينسّق إعادة توزيع المهام أو إسنادها إلى زميل احتياطي. النجاح الفعلي لهذا النظام قائم على الثقة بعدم استخدام هذه المعلومات لإدانة الموظف، بل لتوفير دعائم وقائية كالتدريب المساعد أو جلسات الاستشارة النفسية. تبيّن الإحصاءات أن شركات الطيران التي فعلت هذا النموذج خفّضت نسب الهفوات الملاحية الدقيقة بنحو 20 % (Bouziane & Latreche, 2025).

تتبنّى المحطات النووية مبدأ "الزميل الرقيب (Buddy System)" حيث يُكلّف كل فنيّ بزميلٍ يراقب أدائه في المهام الحرجة ويتعاون معه في تطبيق قوائم الفحص. الفارق عن الرصد التلقيني هو اتفاق مسبق على تبادل النصائح والتذكير اللطيف في الوقت الحقيقي، بحيث يصبح كل فرد مسؤولاً عن سلامة الآخر لا عن سلامته الفردية فقط. تشير الأدبيات إلى أن هذا الأسلوب يعمّق شعور الانتماء ويعزّز الاتكال المتبادل ضمن الحدود الآمنة، ما يقلل من ميل الفرد لتخطي إجراء أثناء ضغط الوقت. في أحد المفاعلات الأوروبية انخفض معدل التقصير في اتباع بروتوكولات الصيانة من 5.2 حالة سنوياً إلى حالة واحدة فقط خلال ثلاثة أعوام من تطبيق النظام. (Laib, 2021)

7.1.2 نظريات "التعويض الخطر" ومواجهة ميل الأفراد إلى الاستهتار

تلفت نظرية "التعويض الخطر" أو "التوازن الأخلاقي" الانتباه إلى سلوك بشري يزداد فيه التهاون كلما شعر المرء بالأمان. على سبيل المثال، قد يقود الموظف رافعة الشوكية داخل المخزن بسرعة أكبر إذا علم أن النظام مزوّد بمكابح تلقائية لمنع الاصطدام، ظانّاً أن التقنية ستحميه من عواقب التهور. ينبّه علماء النفس الصناعي إلى ضرورة مواكبة كل تحسين تقني بحملة توعوية تكشف حدود النظام وتظهر أن الاعتماد التام على الأتمتة قد يُولّد ثغرة أشدّ خطورة. وعليه، صممت بعض مصانع تجميع الإلكترونيات "دروساً عكسية" تحاكي تعطيل مؤقت للمستشعرات، ما يدفع العامل إلى استشعار الخطر عياناً ويتذكر عن كثب

أن التكنولوجيا ليست عصا سحرية لمعالجة كافة الأخطاء البشرية. (Metwally, Abdelazim & Almarji, 2022)

مثلما يرتدي العامل في موقع البناء خوذة وسترة عاكسة، طُرحت حديثاً فكرة "المعدات الوقائية النفسية" في البيئات شديدة التوتر. تتمثل ببرامج وأدوات رقمية تقدم "استراحتين ذهنتين" على مدار الوردية، يتلقى فيها الموظف تدريباً مصغراً في تقنيات تهدئة الجهاز العصبي، مثل التنفس الإيقاعي أو التخيل البصري لمكان آمن. تُختبر حالياً في مستودعات شحن عملاقة تعاني من نسب دوران وظيفي مرتفعة. تشير النتائج الأولية إلى أن الجلسات النفسية المجدولة تُخفف عبء الضغط اليومي، وتحمي من الانفجارات الانفعالية المرتبطة بالأخطاء الحرجة، كما تُشعر العامل بأن المؤسسة تعتني بسلامته النفسية لا الجسدية فحسب. (Badran, Abdel Gaber & Haggag, 2024)

8.1.2 إيقاع المناوبات الذكية وإنصاف الساعة البيولوجية

تفرض بعض الصناعات نظام المناوبات المتداخلة على مدى 24 ساعة، لكن عندما لا يُصمَّم الجدول بما يتوافق مع الساعة البيولوجية للفرد ترتفع نسبة الحوادث الليلية بشكل ملحوظ. طوّرت شركات الطيران نهجاً يسمى "المناوبات الذكية"؛ يُخضع الموظفون لتقييم بسيط يكشف ما إذا كانوا يُعرّفون بـ "البوم الليلي" أو "الطير الصباحي". بعد تحليل نتائج الفريق بالكامل تُبنى الجداول بنمط "التحليق بالمواهب" فيوضع أصحاب النشاط الليلي في المناوبات المتأخرة وينتقلون تدريجياً إلى ورديات نهائية أقل إجهاداً. هذه الملاءمة البيولوجية حدّت من حوادث النوم القصير على أجهزة التحكم بنسبة 35 % في وحدات الملاحة الإسكندنافية، حيث يُعدّ دوام الليل عادةً المصدر الأكبر للأخطاء البشرية المرتبطة بالنعاس. (Salim & Khammas, 2023)

لا تنفصل المخاطر البشرية الناشئة عن المشكلات الخاصة كالمصاعب المالية أو الأزمات العائلية. لذا باتت الشركات الكبرى تستثمر في "البرامج المساعدة للموظفين" (Employee Assistance Programs) التي تقدّم استشارات مجانية أو مدعومة في الجوانب النفسية والقانونية والمالية. تكشف البيانات أن الموظف الذي يمر بضائقة شخصية يكون أكثر عرضة للوقوع في الخطأ المهني بنسبة تصل إلى 45 % إذا لم

يُقدّم له دعم مناسب. وتجدر الإشارة إلى أن أغلب الموظفين لا يعلنون عن ظروفهم الخاصة إلا في بيئة "أمان نفسي" يشعرون فيها أن البوح لن يعرضهم للوصم أو العقاب. (Al-Salahi & Al-Tarawneh, 2024) عندما فعلت إحدى شركات النقل البحري برنامج المساعدة، هبط معدل الأخطاء التشغيلية خلال تسليم الحاويات بنحو 14 % خلال عامين.

ترتبط إدارة السفن بعوامل بشرية معقّدة، إذ تعيش الأطقم لشهور طويلة في بيئة مغلقة ويتصاعد الإحساس بالعزلة. ظاهرة "التمرد الصامت" تُطلق على امتناع البحارة عن الإبلاغ عن الأخطاء الصغرى أو تعمدّهم تعطيل إجراءات روتينية بسبب احتقان مكنون. طوّرت إحدى شركات الملاحة العالمية نظام "منتدى آمن" يُقام مرة كل أسبوعين على متن السفينة، يُدار بواسطة مسؤولين مكلفين من خارج سلسلة القيادة الرسمية، لتشجيع النقاش حول الصعوبات الفنية والنفسية بلا خوف من انتقام القبطان أو ضابط أول. بيّنت تقارير الشركة أن حالات انهيار التعاون أثناء الطقس العاصف تراجعت بمعدل 30 % لأن الفريق اكتسب متنبساً منظماً للتنفيس عن التوتر، ما قلّل من الأخطاء الارتجالية تحت الضغط المفاجئ. (Ramadan, 2022)

9.1.2 المؤشرات القائدة في السلامة مقابل المؤشرات التابعة

ت historically relied heavily on مؤشرات "تابعة" (Lagging Indicators) "مثل عدد الإصابات أو الحوادث التي وقعت فعلاً، وهي مهمة لكنها لا تساعد في استباق المخاطر. دخلت حالياً مؤشرات "قائدة" (Leading Indicators) تُقيس عوامل استباقية كعدد مرات إجراء عمليات التفتيش المفاجئة، أو نسبة التزام الموظفين بالحضور الكامل في دورات التدريب الدورية، أو درجة انخراطهم في محاكاة الطوارئ. تبدأ إدارة العامل البشري بتعزيز هذه المؤشرات القائدة لتحريك الثقافة قبل وقوع الحادث. كان هذا التحول عميقاً في مصافي النفط الأمريكية حيث أدى التركيز على قياس "مدى تشاركية الفريق في تدريبات الإغلاق والوسم" إلى انخفاض قدره 25 % في الحوادث الجدية خلال عام واحد، لأن كل نقطة في المؤشر القائد عكست تغييراً ملموساً في السلوك. (Abdul Jader, 2022)

في الماضي كانت التحقيقات بحوادث العمل تُغلق فور صدور التقرير النهائي، ما يحرم المؤسسة من حياة متجددة لتلك الدروس. أما الآن فتطفو أهمية "بنوك الدروس المستخلصة" (Lessons Learned Repositories) حيث توثق كل حادثة مع تحليل جذورها، وتُستضاف في منصة تفاعلية تُشجع الموظفين على إضافة تعليقات أو إضافات لأحداث شبيهة. عندما يواجه عضو فريق مشكلة مشابهة، يطلع أوتوماتيكياً على صناديق المعرفة السابقة، ومن ثم ينخرط في "تحقيق تعاوني" حيث يجري تحديث البرنامج التدريبي بناء على التحديات المستجدة. طبقت شركة هندسة معمارية هذه الفكرة عبر تطبيق جوال يرسل تنبيهات حال تطابق صورة التصدع في الهيكل مع نمط حادث سابق في قاعدة البيانات، فجنبت المشروع أضراراً تقدر بملايين الدولارات. بهذا تتحول إدارة مخاطر العامل البشري من نظام رد فعل إلى نظام تعلم حي ومتجدد. (Awad & Al-Khazaali, 2022)

في فلسفة التصنيع الرشيق على استحالة وقوع الخطأ بدلاً من تصحيحه لاحقاً. تتبنى بعض المصانع طرقاً بسيطة لكنها فعالة، مثل استخدام أدوات مصممة بطريقة تمنع تركيب الأجزاء الخطأ في المواقع الخطأ، أو مفاتيح لا تلائم سوى الصمام الصحيح. وقد طوّرت شركات الإلكترونيات نماذج حاضنة ترتبط فيها الأجزاء إلكترونياً برمز استجابة سريع (QR) يمنع العامل من تركيب القطعة إن لم تتطابق مع وسم المحطة. وعلى الرغم من أنّ هذه الأساليب تُقلّل مجال تبادل الخبرات التقليدي بين العمال، فإنها تحدّ جذرياً من أخطاء "النسيان" أو "التشابه البصري" التي هي الأكثر شيوعاً، ما يُحوّل إدارة المخاطر البشرية إلى عملية تصميمية تستبق سلوكيات الإنسان وتوجّهها بحلول هندسية مدروسة. (Attia, Obaidat & Al-Saghir, 2024)

10.1.2 استراتيجيات التصحيح الفوري ونافذة الذهب

تظهر دراسات حوادث البناء أن أمام الموظف المستشعر للخطر مهلة قصيرة لا تتجاوز ثواني معدودة لاستباق الخطأ قبل تحوُّله إلى حدث فعلي. يسمّيها بعض الخبراء "نافذة الذهب" (Golden Window) حيث يكون ردُّ الفعل المبكر حاسماً في تجنب خسائر فادحة. طوّرت شركات الإنشاء الكبرى بروتوكولاً يمنح الموظف سلطات تنفيذية حتى لو كان في أدنى الدرجات الوظيفية؛ فإذا لاحظ عملية رفع

غير مستقرة يحقّ له إيقاف الرافعة فوراً بغضّ النظر عن اعتراض المشرف. ثم تُعقد جلسة سريعة مع الفريق للتدقيق في سبب الإيقاف. هذا النهج، بالرغم من أنّه قد يزيد عدد المقاطعات الظاهرية، فإنه خفّض الحوادث الجسيمة بنسبة خمسين بالمائة في إحدى الشركات خلال عام، وأثبت أن تقدير دور الإجراء الفوري يعزز السلوك الوقائي. (Al-Tarawneh, Al-Jubouri & Al-Maaytah, 2020)

يتعاون متخصصو السلوك مع علماء البيانات لتطوير "حساسيات القرار (Decision Sensitivities) في البيانات التي تعتمد على التخطيط الاستشرافي. في شركات الخدمات اللوجستية العالمية، يُنشئ فريق الذكاء الاصطناعي نموذجاً محاكياً لحركة الشحن والتوصيل مع عامل إضافي: احتمالية الخطأ البشري عند كل نقطة اتصال أو تسليم. يأخذ النموذج بالاعتبار عوامل مثل الإرهاق في نهاية الوردية، واختلاف اللغات بين الموظفين، وحتى تأثير الأحوال الجوية على المزاج. والنتيجة هي "خريطة حرارية حية" توضح تصاعد نسبة الأخطاء في بعض الأيام أو المدن. وبفضل هذه الخريطة، تُوجّه حملات دعم إضافي أو تُعدّل جداول العمل استباقياً في المناطق الساخنة. بهذا تتحوّل إدارة المخاطر من ردّ فعل بعد وقوع الأخطاء إلى إدارة توقعيه تواكب ديناميكية العمليات المعقّدة. (Debbache, Roula & Benfenatki, 2023)

أحد أبرز جوانب المخاطر البشرية هو الانقطاع المعرفي الذي يحدث عندما يُنوّه في دليل التشغيل إلى استثناء لا يقرأه الموظفون أو يتجاهلونه بسبب ضيق الوقت. تسمّى هذه العتبة "نقطة التحول" في التعليمات، حيث يجب على الفرد الانتقال من "الوضع التلقائي" إلى "الوضع الحذر. (Alert Mode) "لجسر تلك الفجوة ابتكرت قطاعات التصنيع تقنية "تعليمات حيّة" تُعتمد فيها وحدات تنبيه تفاعلية؛ يعتمد النظام على حساس أو كاميرا تدرس وضعية يد العامل أو حركته، ثم ينبثق مقطع فيديو قصير يشرح الخطوة الخطرة أو الاستثناء في ثوانٍ. فبدلاً من كتابة نص مطوّل قد لا يُقرأ، تُعرض المعلومة المطلوبة فوراً في اللحظة المناسبة. بالتطبيق على مصانع الأدوات الطبية، انخفضت أخطاء تبديل القوالب في مرحلة التعقيم 30% خلال نصف سنة. (Hamed, 2023)

تصف الأدبيات مصطلح "التكيّف الأخلاقي" حين يتعرّض الموظف لمخالفات طفيفة متكررة تتحوّل مع الوقت إلى ممارسة نظامية. فمثلاً، يحمل الطيّار فائض أمتعة عن الحد القانوني بضعة كيلوغرامات

اعتقاداً بأن الأمر بسيط، ثم تتراكم تلك الكيلوغرامات عبر الرحلات لتصل إلى حد خطر. تعتمد شركات الطيران منهج "التدقيق المفاجئ على الصغائر" للحد من الاعتیاد غير الصحي، فيهيّط مفتش متخصص في مطار غير رئيسي أو أثناء محطة عابرة ليفحص تطابق الحمولة الفعلي مع السجل ومقارنة قوائم المسافرين بالوزن الحقيقي. من خلال هذه المراجعات العشوائية المنتظمة يُهدم مفهوم "المعتاد" ويُعاد ترسيخ ثقافة الالتزام الدائم بالإجراءات. وقد كشفت إحصائيات إحدى الشركات أن معدل الحمولة الزائدة انكمش إلى الصفر تقريباً خلال 18 شهراً بعد تطبيق البرنامج. (Maqbul, 2024)

في مهام تتطلب تركيزاً عالياً على المدى الطويل، يستهلك الإرهاق الذهني قدرات الفرد تدريجياً. لمواجهة ذلك، ابتكرت بعض الشركات مفهوم "صرف الانتباه المسيطر (Controlled Distraction)"; يُسمح للموظف العامل في مهمة رتيبة وحرّة—مثل مراقبة الشاشات الأمنية أو عدّ أدوية في صيدلية مركزية—بالخروج كل ساعتين إلى ركن ترفيهي مصغّر يؤمّن له استراحة ذهنية في ثلاث إلى خمس دقائق فقط. المفتاح هو مواصفات المكان: شاشة تعرض مشاهد طبيعية متغيرة، مع أصوات بيئية هادئة، ولا وجود للتعليقات الاجتماعية أو الأخبار المقلقة. وفقاً لدراسة بالقطاع الصحي البريطاني، أدّى اعتماد هذا الأسلوب إلى خفض الأخطاء الصيدلانية بنسبة 28% وإلى ارتفاع رضا العاملين بشكل ملحوظ، إذ شعروا بقدرة أكبر على استعادة التركيز دون الشعور بالذنب بسبب التوقف القصير. (Al-Ramadan et al., 2022)

11.1.2 الكشف المبكر عن "مستودعات الغضب" بين الفرق

عندما تتراكم خلافات صغيرة بين الأقسام أو فرق العمل من دون حلّ جذري، تنشأ بؤر تسمّى "مستودعات الغضب (Anger Depots)" تضغط على الأفراد وتزيد احتمال حدوث أخطاء ناتجة عن انتقام أو إحباط جماعي. تراقب الشركات الرائدة منصّات التواصل الداخلي لرصد مفردات ذات شحنة سلبية عالية أو ارتفاع مفاجئ في استخدام رموز المشاعر الغاضبة. عند تجاوز عتبة معيّنة تتولّى لجنة مصالحة داخلية عقد "شهور سلام" تتضمن ورش تشاركية ومسابقات ودّية لتفريغ الطاقة السلبية وتكوين علاقات إيجابية جديدة. وفعلاً، في إحدى شركات تقنية المعلومات انخفضت "الحوادث المعرّقة" الناشئة عن رفض

التعاون 40% في الربع التالي لإطلاق برنامج المصالحة الذكي، ما يدل على أن مراقبة الأجواء العاطفية ليست ترفاً بل وسيلة للسيطرة على المخاطر الخفية. (Al-Balawi, 2025)

تخشى منظمات عدة من تشجيع التجريب خشية وقوع الأخطاء. إلا أن نموذج "بيئة التعلم العميق" يتيح قدرًا من التجريب المنضبط في سياقات محددة. في هذه البيئة، يُسمح للموظف بتطبيق فكرة جديدة—كأسلوب تشحيم مختلف في خط إنتاج أو منهجية توزيع بضائع مبتكرة—على نطاق ضيق دون عقوبة إن لم ينجح. شرط ذلك هو التوثيق المسبق: وضع افتراضات، وتقدير احتمالية الخطأ، ووضع خطط لتطويق الأثر. إن وقع الخطأ فعلاً، تُعقد جلسة لمناقشة الأسباب والمنفعة من نتائجه. وفي حالة نجاح الابتكار تنشره الشركة على نطاق أوسع. هذا الأسلوب عزّز لدى إحدى شركات المنتجات الاستهلاكية روح المبادرة الخلاقة وخفّف إخفاء الأخطاء، وجعل المؤسسة أكثر استعداداً لاحتمالات الفشل البشري الإيجابي—أي الفشل الذي يفتح نافذة لتطوير النظام بمجمله. (Dohi, 2024)

أصبح البُعد الاجتماعي في الاستدامة مكوناً معترفاً به إلى جانب الأبعاد البيئية والاقتصادية، ما فتح المجال لدمج إدارة المخاطر البشرية ضمن برامج المسؤولية الاجتماعية للمؤسسات. فبدلاً من التركيز حصراً على حماية العامل من الإصابات، ينصبّ الاهتمام على جودة حياة الموظف وأسرته ومجتمعه المحلي. تُشيد بعض الشركات مرافق رعاية الأطفال بالقرب من مواقع العمل الخطرة بهدف تخفيف الضغط الأسري الذي قد يزيد احتمالات الغفلة أو التسرع. بفضل هذه المرفقة الاجتماعية هبط معدل الإصابات الخفيفة في منجم نحاس بإحدى الدول الإفريقية 32%، كما تحسّنت سمعة الشركة محلياً لاهتمامها بالسلامة والاستقرار الأسري للعاملين. هذا الارتباط بين الإدارة الوقائية والمساهمة المجتمعية يطور "ترابطاً نفسياً" يجعل قيم السلامة والأمان جزءاً من هوية المؤسسة في الداخل والخارج. (Abu Alead & Ab, 2023)

لدى القطاعات التي تواجه تهديداً آنياً—كالعمليات العسكرية أو خطة إخلاء المنشآت الكيميائية—ثوانٍ معدودة لاتخاذ قرارات مصيرية. تطبق هذه المؤسسات مفهوم "الاستعداد السلوكي" (Behavioral Preparedness) عبر تمارينات خاطفة Micro-Drills تُكرّر كل أسبوعين، تستمر بضع دقائق

فقط، وتحاكي الانفجارات المفاجئة أو تسرب الغاز أو إنذار حريق. الهدف هو برمجة النظام العصبي للموظفين للانتقال فوراً لحالة "الاستجابة الواعية" (Conscious Response) "دون التشويش الذي يرافق الصدمة الأولى. وقد نجحت مديرية الدفاع المدني في إحدى العواصم المكتظة بتخفيض زمن إخلاء الأبراج إلى النصف بعد سبعة أشهر من اتباع هذه التدريبات، ما يعكس قوة ترسيخ المسارات السلوكية السريعة في خفض المخاطر الناتجة عن التردد. (Al-Muadat, Bani Ahmed & Al-Durgham, 2023)

12.1.2 دراسة "الحوادث الإيجابية" ورصد النجاح المنقذ

لا تقتصر ثقافة السلامة على فحص الأخطاء وحدها؛ إذ إن تعلّم ما تم فعله على نحو صائب في لحظة حرجة لا يقل أهمية. في الحوادث الإيجابية (Positive Incidents) ينجح العامل أو الفريق في منع الكارثة عبر موقف استثنائي أو إجراء مبادر. تؤثّق هذه الوقائع بطريقة محاكاة متعمّقة تشبه التحقيق، لكن بدل توجيه الأسئلة حول "لماذا حدث الخطأ؟"، يُسأل الموظف: "كيف عرفت التصرف بهذا الشكل الصحيح؟ ومن أين اكتسبت المعلومة؟". تُحلّل تلك الأجوبة لاستخلاص الدروس التي يمكن تحويلها إلى أداة تدريبية عامة، لتنتشر الحلول المبتكرة بدل بقاءها طي الخبرة الفردية. أثبتت هذه المنهجية في شركات الصيانة البحرية أنها تعزّز التفاؤل الجمعي وتشجع الموظفين الآخرين على المبادرة عند مواجهة مخاطر مفاجئة. (Al-Tamimi & Mughaid, 2024)

تبيّن الأبحاث السلوكية أن الاعتماد على أسلوب العقاب أو الزجر وحده قد يخلق جواً من الخوف والتسرّب على الأخطاء، فيعيق الإبلاغ المبكر ويغذي الإهمال الخفي. بالمقابل، يشيره علماء النفس إلى أن أسلوب تعزيز السلوك المرغوب عن طريق الثناء أو المكافأة الرمزية يحفّز الأفراد على الاقتداء بالإجراءات السليمة. فتقديم جائزة بسيطة للموظف الذي رصد مخاطرة وبلغ عنها يُبني فخره بالمشاركة في توكّي السلامة ويشجع زملاءه على الحذو حذوه. وفي مؤسسات رائدة، تُنشأ لوحات شرف علنية تُكرّم بها الفرق التي حققت سجلاً نظيفاً من الأخطاء خلال فترة معينة. هذا الانتباه للسلوك الإيجابي يرسّخ ثقافة بأن الوقاية ليست واجباً إلزامياً فحسب، بل هي مصدر تقدير واعتزاز شخصي وجماعي. (Al-Quraan & Obaidat, 2023)

لا يمكن لممارسات السلامة أن تنبئ وتؤتي ثمارها إن لم يؤمن القادة أنفسهم بقيم إدارة مخاطر العامل البشري، ويتصرفوا بما يعكس ذلك النهج في التوجيه والمتابعة. في كثير من الأحيان، يظهر انفصام واضح عندما تسارع الإدارة الميدانية للوم الموظف بعد حادث، بينما تُرسل الإدارة العليا إشارات عكسية تُجبره على التساهل مع إجراءات التشغيل لإبقاء عجلة الإنتاج. لذا من الضروري بناء قنوات تواصل شفافة تشجع الموظفين على إبلاغ الإدارة بأي ضغط عمل يجبرهم على خرق قواعد السلامة. وعندما تتماسك القيادة وتُظهر تضامناً حقيقياً في حل المشكلات الجذرية، لا سيما تلك المتصلة بالتخطيط الزمني أو كثافة العمل غير الواقعية، فإن ذلك يساهم في بناء مناعة تنظيمية تصون إيقاع الأداء السليم. (Albalushi, Ali & Aman, 2022)

تحدث أحياناً حوادث أو أخطاء جسيمة بسبب الاعتماد المفرط على موظف واحد يمتلك خبرة فريدة أو يسيطر على معلومة حاسمة. في مثل هذه البيئة، قد ينغلق ذلك الشخص على أساليبه الخاصة وقد لا يشارك ما يعرفه مع فريقه، ما يضاعف المخاطر إن غاب لأي سبب أو وقع تحت ضغط نفسي. لإدارة مثل هذه الثغرة، تعتمد بعض المؤسسات نظام التناوب الدوري بين الوظائف المتشابهة، بحيث يتعلم كل فرد مهام زميله على الأقل بالحد الكافي لتشغيل الطوارئ. هذه الآلية تحفّز نقل المعرفة وتمنع تضخم مخاطر "الشخص الوحيد" (Single Point of Failure) "إلى جانب ذلك، تُشجّع عمليات تدوين المعلومات الحساسة في أدلة عمل واضحة ومحدّثة تسهّل عمليات المراجعة والمتابعة عند غياب الموظف المسؤول. (Ahmed, Kazar & Harous, 2024)

لا تنفصل إدارة مخاطر العامل البشري عن الحالة النفسية والعاطفية للموظفين؛ فالشخص الذي يعاني توتراً مزمناً أو مشاكل عائلية حادة قد ينخفض مستوى تركيزه وتزداد قابلية ارتكاب أخطاء كارثية. في السابق، كان الرقم المعتبر هو الأيام المرضية الجسدية، أما اليوم فتبرز مؤشرات مثل تغيّرات المزاج والإجهاد النفسي كعوامل تنعكس على معدلات حوادث العمل. لذا فإن توفير استشارات الدعم النفسي أو خط مساعدة سري يعنى بتفريغ الضغوط يساهم بوضوح في تقليص الحوادث. زد على ذلك، تزداد بعض المؤسسات توفير مساحات هادئة للاستراحة الذهنية وتطبيق برامج قصيرة للتنفّس الواعي

(Mindfulness) خلال نوبة العمل، ما يضيق فجوة الإرهاق ويحقق توازناً أفضل بين البُعد الإنتاجي والإنساني. (Bouziane & Latreche, 2025)

يشكل التصميم السيئ للأدوات والمعدات أحد أهم العوامل التي تقود للأخطاء البشرية. حين يكون واجهة الماكينة معقداً أو بلغة لا يفهمها الموظف، وحين تتشابه مقابض التشغيل المتاحة دون تفرقة لونية واضحة، تتصاعد احتمالية تشغيل الخانة الخطأ. هنا تساهم "الهندسة البشرية (Human Factors)" (Engineering) في تكييف بيئة العمل لتناسب القدرات البشرية، مثل توزيع الإضاءة وتوجيه الأصوات وتحسين الواجهات الرقمية كي تكون بديهية ومنخفضة التعقيد. ومن أبرز الأمثلة نجاح مختبرات الطيران في تقليل حوادث الهبوط الاضطراري من خلال إعادة تصميم أزرار القمرة وإبراز الإشعارات الأكثر أهمية في مكان مميز. يتطلب ذلك التعاون الوثيق بين المهندسين والمختصين بالسلوك البشري لمعالجة التحديات التصميمية بدقة. (Laib, 2021)

تتسع رقعة المخاطر البشرية عند تزاوج العمل التقليدي بالمنصات الرقمية، حيث يتعرض الموظف ربما لفيض مستمر من التنبيهات ورسائل البريد الفورية، ما يزيد تشتته ويخفض إنتاجيته ويرفع فرص ارتكاب أخطاء. يضاف إلى ذلك التطور الكبير في نظم الأتمتة التي قد تورث الموظف إحساساً بالثقة المفرطة فيها. ومن هنا تبرز أهمية إشراك فرق تقنية المعلومات في تصميم عناصر التحكم السلوكي على الأنظمة، مثل إجبار المستخدم على التحقق المزدوج قبل إرسال بريد جماعي أو الموافقة على صفقة مالية ضخمة. وتساعد هذه "حواجز الأمان" الرقمية في كبح القفز المتهور نحو القرارات الحرجة، وتمنع من الوقوع في شرك اللحظة غير المنضبطة. (Metwally, Abdelazim & Almarji, 2022)

لضمان عدم اتساع هامش الخطأ البشري، تُنشئ بعض المؤسسات نظاماً للرقابة الاستباقية قائم على "مؤشرات مخاطر رئيسية (Key Risk Indicators)" سلوكية. فتتابع مثلاً معدل تغيب الموظفين، أو جِدّة النبرات في رسائل البريد الداخلي، أو زمن الاستجابة للأعطال المفاجئة. تجمع هذه البيانات وتُحلل بالاستعانة بتحليلات متقدمة لتوفير إنذار مبكر قبل تحول حالة سوء الانضباط أو الإجهاد إلى حوادث فعلية. ويلزم بالطبع الالتزام بأخلاقيات الخصوصية والشفافية عند جمع بيانات الموظفين، بحيث يكون

الهدف وقائياً بالأساس وليس أداة للتجسس أو العقاب العشوائي. هذه النماذج التي بُنيت على علم البيانات السيكلوجي أثبتت قدرتها على التنبؤ بقابلية انهيار الأداء أو تصاعد النزاعات بين أفراد الفريق. (Badran,

(Abdel Gaber & Haggag, 2024)

13.1.2 الذكاء الاصطناعي في خدمة الحد من الأخطاء البشرية

مع انتشار الذكاء الاصطناعي وتعلّم الآلة بات ممكناً تحليل كميات ضخمة من البيانات التي تنتجها بيئة العمل، سواءً البيانات الحسية أو النصية. هذا يفسح المجال لتطوير نظم تتبع الأخطاء شبه المؤكدة، وبناء خرائط مخاطر متداخلة توضح العلاقات الخفية بين سلوك الموظف وظروف بيئة العمل. فعلى سبيل المثال، قد يكتشف النظام أن خطأ تشغيلياً يزيد بشكل خاص حين تتجاوز درجات الحرارة في المصنع حداً معيناً أو تتكرر شكاوى الموظف في تلك الفترة الانتقالية بين ورديتين. كما تُعدّ روبوتات المحادثة (Chatbots) الداخلية وسيلة لدعم الموظف عند البحث عن معلومة أو إجراء معيّن، فتوجهه فوراً نحو دليل العمل المناسب أو تزوده بتنبيهه إذا بدا على وشك تخطي قاعدة أمان. بهذا تُوظّف التكنولوجيا المعرفية للوقاية من الزلات البشرية قبل حدوثها. (Salim & Khammas, 2023)

لا تنتهي دورة إدارة مخاطر العامل البشري بالمنع؛ فإذا وقع حادث بالفعل، ينبغي أن تُجرى تحقيقات عالية الشفافية تركز على العامل النظامي لا الشخصي. يُعرف هذا التوجه بأسلوب "الثقافة العادلة" (Just Culture) حيث لا يُعاقب الموظف على خطأ غير متعمد، بل تُشخّص الأسباب سواء كانت نقصاً تدريبياً أم ضغطاً زمنياً أم قرارات إدارية دفعت لإهمال المعايير. ثم تُخطط دورة تعلم تغلق الحلقة عبر تحديث الإجراءات أو توفير دعم إضافي لضمان عدم تكرار الحدث. وعندما تنتشر هذه الروح المنصفة، لا يعود الموظفون يخشون الإبلاغ السريع عن الأخطاء أو الحوادث الوشيكة. (Ismail, 2020)

المبحث الثاني: الهجمات السيبرانية

1.2.2 المقدمة

تُعدّ واحدة من أخطر الظواهر الأمنية المعاصرة، إذ تنتقل بها الجرائم التقليدية إلى فضاء رقمي مليء بالتعقيدات التقنية والتهديدات متعددة الوجوه. يتمحور مفهوم "الهجمات السيبرانية" حول أي نشاط عدائي يستهدف الأنظمة الإلكترونية أو البنى التحتية الرقمية بهدف تعطيلها أو سرقة بياناتها أو اختراقها لتحقيق مكاسب مالية أو سياسية أو حتى انتقامية. وتشمل هذه الهجمات مجموعة واسعة من الأساليب، من استغلال الثغرات البرمجية واستخدام برامج الفدية (Ransomware) وصولاً إلى عمليات التصيد (Phishing) التي تسعى لخداع المستخدمين وسرقة هوياتهم الرقمية. ما يجعل هذا المشهد أكثر تعقيداً هو تنامي مهارات القراصنة وصعوبة تحديد هويتهم الحقيقية، إذ يمكن إدارة الهجمة من خلال شبكات افتراضية (VPN) أو باستخدام برمجيات التخفي بحيث يصعب تتبع المصدر الفعلي . (Al-Salahi & Al-Tarawneh, 2024)

يمهّد هذا المناخ لظهور هجمات منظمة تقف خلفها جهات حكومية أو مجموعات قرصنة شديدة التنظيم تُعرف باسم التهديدات المستمرة المتقدمة (Advanced Persistent Threats - APTs) تتخذ هذه المجموعات من القدرة على التخفي واستمرار التسلّل ركائز أساسية، حيث تدرس الهدف بدقة وتنتظر اللحظة المناسبة لتنفيذ الهجمة أو سرقة البيانات دون إثارة الانتباه. وغالباً ما يستهدفون القطاعات الحساسة مثل الطاقة أو البنى التحتية المالية بغية إحداث اضطراب شامل، أو تجميع معلومات استخباراتية على مدى زمني طويل. (Al-Dhawadi, 2020)

يواكب ذلك تزايد مقلق في عدد الثغرات "اليوم الصفري" (Zero-Day Vulnerabilities) التي لا يتوفر لها بعد أي تحديث أمني من الشركات المطوّرة، مما يمنح المهاجمين فرصة ذهبية للولوج إلى شبكات الضحايا قبل أن يتمكنوا من سد هذه الفجوات . (Ramadan, 2022)

إلى جانب الهجمات المتطورة، لا يزال العنصر البشري أحد أضعف حلقات الدفاع في سلاسل الأمن السيبراني. إذ غالباً ما يتعرض الموظفون عن غير قصد لرسائل بريد خبيثة تبدو رسمية، أو ينقرون على

روابط تقود إلى صفحات ومواقع مُزوّرة، في عملية تُعرف باسم التصيّد الاحتيالي. وعند تدوير كلمات مرور بسيطة أو تكرار استخدامها في أكثر من موقع، تتضاعف فرص نجاح المهاجمين في انتزاع حقوق وصول أعلى يمكنهم بواسطتها التنقّل بحرية داخل البنية التحتية. ويلجأ المخترقون في أحيان كثيرة إلى تكتيكات الهندسة الاجتماعية، مستغلّين فضول المستخدم أو خوفه لإقناعه بتسهيل العملية؛ فبمجرد التعرف إلى ثغرة في سلوك بشري أو ناموس تنظيمي، يستطيع القراصنة التحكّم في الأنظمة وسحب ما يحتاجونه من بيانات أو حتى تدميرها.

تمتد آثار الهجمات السيبرانية أفقياً وعمودياً، فتُلحق ضرراً في جوانب قد تفوق الخسائر المالية المباشرة. ففي حال اختراق مرافق صحية مثلاً، لا يقتصر الخطر على المساس بخصوصية المرضى وسرقة بياناتهم الكبرى، بل قد يمتد ليعطل أنظمة دعم الحياة أو الأجهزة الحرجة في غرف العناية. يتشابه الأمر في قطاعات حيوية أخرى كالمطارات والمرافق الحكومية، حيث تؤدي الهجمات أحياناً إلى شلل في الخدمات الأساسية أو شيع حالة من الذعر العام. (Abdul Jader, 2022)

وطالما تحدث هذه الاختراقات على نطاق واسع، تزداد معها احتمالية الإضرار بالسمعة المؤسسية وفقدان ثقة العملاء أو المستثمرين. وفي بعض الحالات قد تتعقّد الأمور أكثر، عندما يتطوّر الأمر إلى دفع فديات مالية بمبالغ طائلة لتجنب نشر البيانات أو إعادة تشغيل الشبكات بعد تشفيرها. (Awad & Al-Khazaali, 2022)

تسعى المؤسسات الضخمة والأجهزة الحكومية على الصعيد العالمي إلى بناء حصون رقمية قادرة على صدّ الهجمات وتخفيف أضرارها اللاحقة؛ فتسنّ تشريعات تُلزم الشركات بإبلاغ الجهات المعنية عن أي اختراق يقع، وتضع معايير للخصوصية وحماية البيانات مثل لائحة الاتحاد الأوروبي (GDPR) في المجال الأوروبي. كما تستثمر بكثافة في برمجيات مضادة للفيروسات، وجدران نارية (Firewalls)، فضلاً عن تقنيات التحليل السلوكي للأنظمة لمراقبة أي نشاط شاذ قد يشير إلى اختراق. لكن رغم هذا التحصين، تظل تلك الأساليب الدفاعية عرضة للتحايل من جانب الخصوم الذين يملكون وصولاً إلى أدوات متطورة في سوق برمجيات الاختراق. وفي مواجهة ذلك، تتجه السياسات الأمنية الحديثة نحو تبني استراتيجية "صفر ثقة"

(Zero Trust) التي تفرض مصادقات متعددة العوامل على كل طلب وصول في الشبكة، وتعامل أي نشاط لا يخضع للتحقق الكامل بوصفه نشاطاً عدائياً محتملاً، في محاولة لتجاوز الاعتماد على الجدران النارية التقليدية وحدها . (Attia, Obaidat & Al-Saghir, 2024)

في هذا المشهد بالغ التعقيد، تتكشف أهمية التوعية والتثقيف الأمني؛ فالمؤسسات التي تدرب موظفيها بانتظام على التعرف إلى الرسائل الاحتيالية وأساليب الهندسة الاجتماعية تقل لديها معدلات الاختراق بشكل ملحوظ. كما يوصي الخبراء بالمراجعة الدورية للإعدادات الأمنية، وتحديث الأنظمة والبرامج بشكل فوري حال صدور ترقيع أمني. ومن جانب آخر، تزايد مبادرات التعاون الدولي في مجال الأمن السيبراني عبر تبادل المعلومات والتحذيرات بشأن هجمات محتملة، مما يعزز قدرة الدول والشركات على التصدي المشترك للتهديدات العالمية المتنامية. ومع اعتماد الاقتصاد العالمي المتزايد على الأصول الرقمية، ستبقى الهجمات السيبرانية تحدياً دائماً لا يمكن احتواؤه إلا بجهد جماعي يزواج بين التكنولوجيا والثقافة الأمنية والسياسات الرادعة. (Al-Tarawneh, Al-Jubouri & Al-Maaytah, 2020)

فيما يلي مجموعة إضافية من الفقرات المطوّلة حول الهجمات السيبرانية، مرفقة باقتراحات لعناوين جانبية يمكن استخدامها لتنظيم هذه الأفكار:

• تصاعد المنحنى التكنولوجي وأثره على تنامي الهجمات

تتطوّر التكنولوجيا بمعدلات مذهلة، فقد غدت عمليات المعالجة السحابية (Cloud Computing) وتقنيات الذكاء الاصطناعي أكثر انتشاراً في شتى القطاعات، مما يوفّر للجهات الإجرامية فرصة لاستغلال هذه القدرات الهائلة في شنّ هجمات أكثر تعقيداً وفعالية. فالبرمجيات الخبيثة اليوم لم تعد تعتمد على أساليب بدائية، بل باتت تستعين بالشبكات العصبونية لتغيير تكتيكات الاختراق، ولتفادي الأنظمة الدفاعية التي تتعلّق بتحليل السلوك. على الجانب المقابل، يصعب على المؤسسات الصغيرة والمتوسطة مجاراة هذه الوتيرة السريعة، بسبب محدودية الموارد والخبرة، مما يضعها في موقع مستضعف غالباً. بالإضافة إلى ذلك، تتعايش معظم الشركات مع واقع "ترابط الأنظمة (System Interconnectivity)"

عبر واجهات برمجية مفتوحة (APIs) تُسهّل التعاون والابتكار، لكنها في الوقت نفسه تُضاعف مساحة التعرض للخطر . (Debbache, Roula & Benfenatki, 2023)

في مشهد التهديدات الافتراضي يمكن التمييز بين هجمات عشوائية يُرسل فيها القراصنة رسائل تصيّد واسعة النطاق أمّلين أن يقع بعض المستخدمين في شركها، وبين هجمات مستهدفة تهدف إلى اختراق جهة بعينها بعد دراسة نقاط ضعفها بدقة. (Hamed, 2023)

الهجمات المستهدفة تعتمد غالباً على تقنيات الهندسة الاجتماعية ومواءمة الرسائل بشكل يبدو مألوفاً ومنطقياً بالنسبة للضحية. وفي بعض الأحيان، يتعاون القراصنة مع خبراء تجسّس تقليديين للحصول على بيانات داخلية تُسهّل عملية الاختحام. أما الهجمات العشوائية فهي أقل تكلفة على المنقّذين، لكنها قد تؤدي إلى إصابات جماعية إذا طالت ملايين الحسابات دفعة واحدة. لهذا تضطر الهيئات الحكومية والقطاع الخاص على حدّ سواء لإعادة تقييم إجراءات الحماية تجاه كلا النمطين . (Maqbul, 2024)

تُعدّ البرامج الضارة بأنواعها المختلفة—الفيروسات (Viruses) ، الديدان (Worms) ، برامج الفدية (Ransomware) ، وبرامج التجسّس—(Spyware) العمود الفقري للهجمات السيبرانية. وتزداد هذه البرمجيات سُميّة مع ظهور “البرمجيات المؤتمتة (Malware-as-a-Service)” المتاحة للبيع أو الإيجار في أسواق الشبكة المظلمة . (Dark Web) ومن أخطر التكتيكات الحديثة اعتماد القراصنة على تقنيات التشفير لتجاوز أغلب برامج الحماية التقليدية، كما يموّهون الفيروسات داخل مكونات برمجية تبدو سليمة. يحدث هذا غالباً أثناء تحديثات البرامج أو الإضافات (Plug-ins) الشائعة التي لا يراجعها المستخدم بعناية. ومن اللافت أن هذه التطبيقات الضارة تتمتع بقدرة على “التحوّل (Polymorphism)” فتغيّر بصمتها الرقمية باستمرار، ما يجعل تتبعها صعباً للغاية ويضع الشركات أمام ضرورة بناء دفاعات سلوكية لا مبنية على التوقيعات الثابتة وحدها. (Al-Ramadan et al., 2022)

بات “إنترنت الأشياء (IoT)” مكوناً أساسياً في الحياة العصرية، حيث أصبحت أجهزة التعدين الذكية والساعات والمركبات وشبكات المراقبة موصولة بشبكة الإنترنت. هذا الترابط يزيد من احتمالية استغلال أي ثغرة صغيرة للتمدد إلى منظومة تقنية أكبر. (Al-Balawi, 2025)

فإذا تم اختراق كاميرا مراقبة ذات تشفير ضعيف، قد يستخدم القراصنة هذا الباب للولوج إلى الشبكة الداخلية في مقر الشركة أو المنزل. وتتفاقم المشكلة عندما تهمل المصانع والمستهلكون على حد سواء تحديثات الأمان دورياً لتلك الأجهزة. فينشأ ما يُسمى "بوت نت (Botnet)" عملاق يجري التحكم به مركزياً لشنّ هجمات الحرمان من الخدمة الموزعة (DDoS) على مواقع محددة، مما يسبّب تعطيلات جماعية في البنى التحتية العامة والخاصة. (Dohi, 2024)

لم تعد الهجمات السيبرانية شأناً تقنياً بحتاً، بل صارت عنصراً قد يُزعزع استقرار اقتصاد بكامله. فالشركات المالية باتت تدفع مبالغ طائلة سنوياً لمكافحة الاختراقات المحتملة وللامتثال للمعايير التنظيمية، ناهيك عن التأمين السيبراني الذي أصبح قطاعاً قائماً بذاته. وفي حال نجح المخترقون في اقتحام أنظمة معقدة، كأنظمة تداول الأسهم أو منصّات التحويل الإلكتروني، قد يتسببون بخسائر اقتصادية جسيمة، أو قد تستخدم هذه البيانات المسروقة في أساليب ابتزاز تنتهي بدفع فديات بمبالغ كبيرة. ولا تقتصر الآثار على الجانب المالي وحده؛ إذ قد تخلّف عمليات الاختراق تداعيات دبلوماسية في حال وُجّهت أصابع الاتهام إلى دولة معينة أو إلى جهة مرتبطة بمصالح عابرة للحدود. (Abu Alead & Ab Altalibe, 2023)

مع توسّع استخدام الذكاء الاصطناعي في شتى التطبيقات، يجري توظيفه كذلك على جبهتي الدفاع والهجوم. فمن جهة، تضيف أنظمة الكشف التنبئي (Predictive Analysis) طبقة جديدة من الحماية تعتمد على تعلّم الآلة لرصد الأنماط الشاذة في الحركة الشبكية، ما يتيح إيقاف التهديد أو عزله قبل حدوث أضرار على نطاق واسع. ومن الجهة الأخرى، قد يلجأ المهاجمون أنفسهم إلى أدوات التعلّم العميق لتوليد رسائل تصيّد مصمّمة بدقّة، أو للبحث عن ثغرات باستخدام روبوتات مسح ذكية. وهكذا تغدو المعركة أقرب إلى سباق تقني تتسارع فيه خطى الابتكار ويتلاشى هامش الخطأ لكلٍ من المهاجم والمدافع معاً، ما يفرض تحديات إضافية على المؤسسات المعنية بتأمين أنظمتها وبناء قدرات متقدمة في التحليل والاستجابة.

(Al-Muadat, Bani Ahmed & Al-Durgham, 2023)

مع ازدياد التهديدات وتعدّد أشكالها، لم يعد خيار الدفاع المنفرد كافياً لمجابهة هجمات تجوب فضاء الإنترنت بلا قيود حدودية. من هنا يتنامى السعي لتشكيل تحالفات دولية تتعاون استخباراتياً وتتبادل

المعلومات الأمنية حول أحدث البرمجيات الضارة وأساليب الاختراق. ويشهد العالم ولادة مبادرات مثل الاتفاقيات المشتركة والتفاهات السياسية بين القوى العظمى لتحديد قواعد الاشتباك السيبراني، على غرار ما يحدث في فضاءات الحرب التقليدية. ورغم أن اتفاقاً دولياً شاملاً يبقى طموحاً صعب المنال، فإن وجود أطر تنسيقية ولو محدودة تساهم بشكل ملحوظ في الإسراع بالتحذير من هجمات محتملة والنظر في سبل الرد على الدول أو الكيانات التي ترعى أو تسمح بممارسات القرصنة الموجهة. (Al-Tamimi & Mughaid, 2024)

لا يمكن تجاهل دور العامل البشري في جميع مراحل الأمن السيبراني. فمهما كانت أنظمة الحماية محصنة، قد تنهار أمام خطأ بشري واحد: كلمة مرور مكررة، أو صفحة تصيد مقنعة، أو جهاز USB مجهول. بدأت كبرى الشركات تطوير "ثقافة أمنية داخلية" تُسهم في جعل كل موظف وظيفياً جزءاً من جدار الحماية الجمعي. يشمل ذلك دورات توعوية تفاعلية تُدرّب الموظفين على تمييز محاولات الاختراق، بالإضافة إلى وضع سياسات واضحة للإبلاغ عن أي حادثة من دون خوف من اللوم. وكثيراً ما تُنثى هذه المؤسسات آليات للمكافآت الرمزية عند اكتشاف ثغرة أمنية أو إبلاغ مبكر عن خطر محتمل، سعياً لترسيخ عقلية "الوقاية المستمرة" بدلاً من مجرد رد الفعل عند حدوث الحادثة. (Al-Quraan & Obaidat, 2023)

خلال السنوات المقبلة، سيشهد المشهد الأمني انتقالاً أكثر كثافة إلى ما يسمى "الحوسبة الكمية" (Quantum Computing) التي تمتلك قدرة هائلة على فك التشفيرات التقليدية خلال وقت وجيز. سيُشكل ذلك تحدياً جذرياً لأنظمة التشفير المستخدمة حالياً في حماية المعاملات المصرفية وتوقيع العقود الرقمية. لذا بدأت بعض الحكومات والمؤسسات العملاقة تحضّر للمرحلة التالية المعروفة بـ "التشفير المقاوم للحوسبة الكمية" (Post-Quantum Cryptography) "كما أن تصاعد الاعتماد على "الواقع الممتد" (Extended Reality) في التطبيقات التجارية والطبية والتعليمية سيضيف حتماً بُعداً جديداً من المخاطر، حيث قد يتم التلاعب بالصور الرقمية للمرضى أو بتجارب الواقع المعزز لإلحاق أضرار بالغة. ومن منظور أوسع، يشير الخبراء إلى أن مواجهة هذه التحديات تتطلب توحيداً دولياً للقوانين وإعداد أجيال ناشئة لديها وعي مبكر بأسلوب الحماية والتعامل المسؤول مع التقنيات الرقمية. (Albalushi, Ali & Aman, 2022)

في نهاية المطاف، تبقى الهجمات السيبرانية واقعاً معقداً ومتجدداً، مما يقتضي مواكبة دائمة على مستوى السياسات والابتكارات التقنية وثقافة المستخدمين على حدّ سواء. إنّ الجمع بين التكنولوجيا المتطورة والتعاون الدولي واليقظة المؤسسية يمثل حجر الأساس لتعزيز مناعة الأنظمة الرقمية، ومنع القرصنة من تحويل مكاسب التحول الرقمي إلى نقاط ضعفٍ مُدمّرة. (Ahmed, Kazar & Harous, 2024)

بدأت ملامح سوق موازية تنمو في الظلام، حيث تعقد فيها صفقات تجارية صريحة لبيع بيانات مخترقة أو تأجير أدوات للتسلل الرقمي. لم يُعدّ القرصنة يُنفذون هجماتهم بمنأى عن الاقتصاد، بل تأسست شبكات منظمة تُسمى أحياناً "بُزوغ الجريمة السيبرانية كخدمة" (Cybercrime-as-a-Service) " في هذه الأسواق يتم توفير "لوحات تحكّم" متكاملة تُتيح لمن لا يمتلكون مهارات تقنية كبيرة نشر فيروسات أو هجمات فدية على نطاق واسع مقابل اشتراك شهري أو نسب عمولة. ونتيجة لذلك، تشهد الإنترنت تصاعداً في عدد الجهات المهاجمة التي تستهدف ضحاياها دون تمييز، وتستخدم موارد مهيكلية بشكل احترافي—من دعم في متوافر على مدار الساعة إلى شروح مكتوبة بلغات متعددة. الأمر الذي يخلق تحدياً مضاعفاً للقوى الأمنية والجهات التنظيمية، إذ يرتفع عدد اللاعبين في ساحة الاختراق ويصبح من الصعب تعقّب المسؤولين الحقيقيين وسط شبكة معقدة من التعاملات السريّة والعملات المشفرة. (Bouziane & Latreche, 2025)

ترافق النمو الكبير في استخدام الهواتف الذكية مع تزايد اهتمام القرصنة باقتحامها، مستفيدين من كونها "جهازاً شخصياً" متصلاً طوال الوقت؛ فكل صور المستخدم ورسائله وحساباته المالية قد تتداخل في تطبيق واحد يتنقل معه أينما ذهب. ولهذا، تزدهر هجمات تُعرف باسم "SMiShing" أو التصيّد عبر الرسائل النصية، إذ يستخدم المهاجم عنوان مرسل يبدو موثقاً، ليجذب الضحية نحو رابط يحتوي برمجيات ضارة. وعندما يستهدف المهاجم أرقام الهواتف—سواء عبر تسريب قاعدة بيانات أو شراء شرائح من سوق سوداء—يصبح الاختراق محتملاً للغاية إذا جرى استدراج المستخدم لتنزيل ملف خبيث. يزيد من خطورة الوضع إعطاء الهواتف وظائف حيوية كاستخدامها في التوثيق الثنائي للهوية أو للوصول إلى محافظ العملات المشفرة؛ فاختراق جهاز محمول قد يمكّن المعتدي من إساءة استغلال كافة المفاتيح الرقمية للمستخدم تقريباً. (Laib, 2021)

أصبحت وسائل التواصل الاجتماعي مسرحاً آخر للهجمات السيبرانية، إذ تُستغل من قبل القراصنة للتجسس وجمع المعلومات الاستخبارية تمهيداً لعملية اختراق أوسع. فالضحية قد يكشف معلومات مهمة عن مكان العمل أو نوع النظام الذي يستخدمه دون أن يعي خطورة ذلك، لا سيما عند نشر صور للشاشات أو معلومات توضح هيكلية الشركة. علاوة على ذلك، انتشرت ظاهرة "ابتزاز السمعة" (Reputation Extortion)، حيث يهدّد المهاجم بنشر صور خاصة أو فيديوهات حساسة على حساب الضحية العام ما لم يدفع مبلغاً مالياً. (Metwally, Abdelazim & Almarji, 2022)

هذه الاستراتيجيات الهجومية تجمع بين الجوانب النفسية وتقنيات الاختراق، ما يستلزم رؤية دفاعية شاملة لا تعالج فقط الإجراءات الأمنية التقنية، بل تمتد إلى سياسات الجرائم الإلكترونية التي تنظّم محتوى التواصل الاجتماعي وتحدّد من التداول العشوائي للبيانات الشخصية. (Badran, Abdel (Gaber & Haggag, 2024

في عالم الهجمات السيبرانية، ثمة فرضية سائدة بأن الهجمات لن تتوقف ما دام هنالك فائدة يمكن تحصيلها. هذا يدفع قطاعات الأمن السيبراني إلى تبني فلسفة "استمرارية التقييم والتكيف"، بمعنى أن منظمة ما لا تكتفي بتدقيق أمني لمرة واحدة أو باقتناء جدار ناري قوي، بل تحتاج بشكل دائم إلى تحديث قواعد بيانات التهديدات وتقييم بيئة عملها التقنية وإيجاد ثغراتها المحتملة. (Salim & Khammas, 2023)

يتضمن ذلك إجراء "اختبارات اختراق" دورية يقوم بها خبراء أمنيون يحاولون تقمّص شخصية القراصنة لاكتشاف نقاط الضعف قبل المهاجمين الحقيقيين. وفي حال اكتُشف اختراق من أي نوع، يجري تحليل مُعمّق لسلسلة الخطوات التي اتّبعتها المهاجم، وتوثيقها في مستودع معرفي يشمل كل خلاصة أو درس يمكن تطبيقه لمنع تكرار السيناريو في المستقبل. (Ismail, 2020)

2.2.2 تنامي دور التأمين السيبراني والخلاف حول جدواه

مع تزايد الهجمات وارتفاع تكلفة الأضرار الناجمة عنها، حلّ التأمين السيبراني بوصفه أداة مالية لتخفيف الخسائر المحتملة. أصبح بإمكان الشركات شراء وثائق تأمين تغطّي نفقات التحقيق في الاختراق

واستعادة البيانات، ودفع الفديات إن اقتضت الضرورة. لكن هذا النهج لا يخلو من جدل، إذ يخشى بعض الخبراء أن تحفيز المنظمات على دفع الفدية قد يشجّع المهاجمين على تصعيد أفعالهم، كما قد تدفع شركات التأمين إلى تحديد أقساط باهظة بعد تراكم طلبات التعويض. (Al-Salahi & Al-Tarawneh, 2024)

يضاف إلى ذلك إشكالية "الأخلاقية السياسية" حين تتورط جهات مؤكّدة بالهجوم، إذ قد تتحوّل أموال التأمين في بعض الحالات إلى مصدر تمويل للإرهاب أو للجماعات الإجرامية. ورغم ذلك، يظل التأمين السيبراني خياراً حيوياً لشركات تواجه مخاطر لا يمكنها تحملها وحدها، مع تأكيد الخبراء على ضرورة أن يُستخدم مع آليات وقائية صلبة لا أن يكون البديل الأوحده للحماية. (Al-Dhawadi, 2020)

غالباً ما تنشط الهجمات السيبرانية في أحلك الظروف، كفترات الاضطراب السياسي أو جائحة صحية مفاجئة. وفي ظل التركيز الإعلامي والمتابعة العامة لهذه الأزمات، قد يستغل القراصنة الوضع من خلال إنشاء مواقع تبرعات وهمية أو حملات تصيد تنتحل صفات منظمات معروفة، جيدة السمعة. كما يمكن أن تنشأ صراعات سيبرانية ضمن الحروب الهجينة بين الدول، إذ تُخطط هجمات تعطيلية تستهدف المستشفيات والمؤسسات الخدمية الكبرى لإرباك الجهة الداخلية لدى الخصم. وعلى الصعيد الاقتصادي، تُدرك المنظمات أن استقرار الصناعات التقنية والتجارية مطلوب أكثر من أي وقت مضى في هذه اللحظات، ما يخلق فرصاً للابتزاز المالي أو السياسي من قبل جهات متورّطة في القرصنة. لذا، باتت الحكومات ترفع جاهزيتها وتحاول وضع بروتوكولات طوارئ سيبرانية على غرار مفاهيم الدفاع المدني التقليدي. (Ramadan, 2022)

لا يقتصر التهديد على النظام الداخلي للمؤسسة وحده، بل يشمل موردي البرامج والأجهزة وشركات الاستشارات التقنية التي غالباً ما تتمتع بحقوق وصول كبيرة (Privileged Access) إذ قد ينفذ المهاجم إلى جهة تعمل مع الشركة المستهدفة ثم يستخدم بيانات الاعتماد المسروقة لاختراق النظام الرئيس. لذلك تتبع بعض الشركات الكبرى ما يسمى "التصديق التكاملي للأمن"، حيث يُطلب من كل مورد تقديم شهادات موثوقة تبرهن التزامه بالمعايير الأمنية، مثل إجراء تدقيق خارجي منتظم على بنيته التحتية التقنية. وفي حالة التعاقد مع مزود موارد بشرية أو خدمات سحابية، تُجبر عقود تتضمن بنوداً صريحة تلزم هؤلاء

المزوّدين بالإبلاغ الفوري عن أي حادث أو ثغرة، وإلاّ تسري عليهم عقوبات مالية تُحفّزهم على تطبيق أعلى معايير الحماية. بهذه الطريقة تحاول المؤسسات تقليص مساحة النفاذ والنقاط الضعيفة على امتداد سلسلة التوريد الرقمية كاملةً. (Abdul Jader, 2022)

تُسهّم العملات المشفرة في طمس هوية المعجريات المالية بشكلٍ جزئي، ما يشكّل وسيلة جذابة للهكرز لتلقي الفدية أو عوائد بيع البيانات المسروقة. ومع أن منصات التداول بدأت تفرض سياسات “اعرف عميلك (KYC)” لتقييد استخدام المحافظ المجهولة، لا يزال بإمكان القراصنة التنقّل بين منصات عدة وتجزئة مبالغهم المالية في محفظات كثيرة لجعل عمليات التتبّع بالغة الصعوبة. وتتجسد خطورة الأمر عندما يجمع المهاجم ما يكفي من أموال الفديات ثم يضخّها في السوق التقليدية عبر قنوات غسيل الأموال. لذلك تبذل الأجهزة الرقابية حول العالم جهداً متزايداً في متابعة حركات التحويل الرقمي، والتحقّق من مشروعية الأرصدة، والقيام بالتحقيقات المالية العميقة لأية معاملات ضخمة أو مشتبّهة فيها. لكنّ الطبيعة العابرة للحدود والعملات اللامركزية يجعل هذه المهمة سلسلة لا تنتهي من المطاردات التقنية والقانونية. (Awad & Al-Khazaali, 2022)

3.2.2 الهندسة العكسية للهجمات ودورها في تطوير أساليب الحماية

بعد تعرّض الأنظمة لأي هجوم سيبراني مهم، قد تختار بعض المؤسسات—إن توافرت لديها الخبرة والموارد—ممارسة ما يُدعى بـ “الهندسة العكسية (Reverse Engineering)” للبرمجيات الخبيثة. أي تقوم بتحليل الكود الضار خطوة بخطوة لفهم آلياته وطرق تشفيره وأهدافه الدقيقة. (Attia, Obaidat & Al-Saghir, 2024)

يساعد هذا الفهم المعمّق على تطوير أدوات مضادة قادرة على كشف الهجوم ذاته في المستقبل، وتحديث قاعدة بيانات التهديدات لدى أنظمة مكافحة الفيروسات. ليس ذلك فحسب، بل يُتيح جمع أدلة جنائية رقمية (Digital Forensics) تساعد أجهزة إنفاذ القانون على تتبّع المهاجمين وتقديمهم للعدالة في بعض الأحيان. ومع ذلك، تتطلّب هذه العملية خبرة متخصصة ووقتاً ليس بالقصير، فضلاً عن الحاجة إلى بيئة تشغيل آمنة للمحللين كي لا يصابوا هم أنفسهم بأضرار. ورغم تعقيدات الهندسة العكسية، فإنها ما

تزال وسيلة جوهريّة تُبقي الخط الدفاعي مواكباً لتطوّر الهجمات. (Al-Tarawneh, Al-Jubouri & Al-) (Maaytah, 2020)

في المجمل، لا يمكن فصل أمن المعلومات في مؤسسات خاصة أو حكومية عن وعي المجتمع ككل، نظراً لما يشكّله المستخدم النهائي من حلقة أساسية قد تكون الأكثر ضعفاً. (Debbache, Roula &) (Benfenatki, 2023)

نظراً لذلك، تتجه بعض الدول إلى تدريس مبادئ السلامة السيبرانية ضمن المناهج الدراسية المبكرة، وإشراك الجمعيات الأهلية في حملات توعية عن مخاطر مشاركة البيانات الشخصية عبر الإنترنت، واختيار كلمات مرور قوية، وعدم الانسياق خلف الروابط المشبوهة. هذا يعكس قناعة متزايدة بأن مجابهة التهديدات الإلكترونية ليست مسؤولية قسم تقنية المعلومات وحده، بل يتطلب "جبهة داخلية رقمية" واعية ومتيقظة لدى عامة الناس. ويضفي تبنى هذه الثقافة على المجتمع حصانة مبتدئة من القاعدة، يتحقق معها حجم أقل من الاختراق وإن كان في سياق توسّع عام للاعتماد على العالم الرقمي. (Hamed,) (2023)

أخذت طبيعة الهجمات السيبرانية منعطفاً جدياً في السنوات الأخيرة مع تكثيف المنظّمات الإجرامية جهودها نحو ما يُعرف بـ"الهجمات الموجّهة"، التي تُستهدف فيها المؤسسات أو الحكومات بعناية فائقة بعد جمع معلومات موسّعة عنها. فقد برزت مجموعات اختراق احترافية—على غرار بعض فرق التهديد المستمر المتقدّم—(APTs) تمزج في عملها بين القرصنة التقنية والتجسس السياسي وسرقة الأسرار الصناعية. في هذه الأوساط، تكون الخطوة الأولى هي الاستطلاع المكثف عبر تتبّع البصمة الرقمية للضحايا والعثور على أكبر قدر من التفاصيل (مثل بنية الشبكة ونقاط الاتصال الحساسة)، ثم تُختار الثغرة المرضية التي يعتقدون أنها الأضعف دفاعاً. تمتاز هذه الهجمات بتخطيطٍ طويل ودؤوب، يتخلله إطلاق برمجيات خبيثة مصمّمة خصيصاً لاستثمار ثغرات فريدة أو لإغراء موظفين معيّنين بالنقر على روابط مفخخة. والأسوأ أن هذه المجموعات تُظهر مهارة بارعة في الاختباء داخل الأنظمة المخترقة فترات ممتدة،

فجمع البيانات وتُراقب حركة الشبكة دون أن تُلاحظ، قبل أن تنفذ الضربة الكبيرة المتمثلة مثلاً في تشفير البيانات أو سرقتها أو تعطيل الإنتاج. (Maqbul, 2024)

باتت البرمجيات الخبيثة (Malware) أكثر تقدماً، منتقلة من فيروسات بدائية تُلحق الضرر بالملفات إلى بوتات هجينة تُوظف تقنيات التعلّم العميق وتغيّر سلوكها أوتوماتيكياً للتهرب من برامج الحماية. من أبرز التطورات دمج خوارزميات تعلّم الآلة في صلب الفيروس، بحيث تستطيع البرمجية استشعار نمط الحماية المنصّب على الجهاز والتكيّف من خلال تعديل بصمتها الرقمية. (Al-Ramadan et al., 2022)

هذا فضلاً عن الأساليب "متعددة الأوجه" (Polymorphic Malware) التي تستطيع تشفير جزمها والمراوغة في أثناء النقل عبر الشبكة. وعلى الجهة المقابلة، تُسارع شركات الأمن السيبراني إلى تطوير أدوات دفاعية تركز هي الأخرى على التحليل السلوكي، حيث تُوظف شبكات عصبية قادرة على تمييز الشذوذ في حركة البيانات. لكن نظراً لأن الحرب السيبرانية أصبحت تدور في بيئة مُعقّدة، تزايد صعوبة اكتشاف الهجمات المبنية على الترابط الذكي، إذ ربما تحتاج المنظّمة إلى تفعيل كثير من المستشعرات الأمنية وتوظيف محركات الاستدلال الفوري على طول الدورة التشغيلية. (Al-Balawi, 2025)

يتزايد قلق الحكومات والشركات حيال تهديد الهجمات السيبرانية للبنى التحتية الحيوية مثل شبكات الكهرباء، ومحطات المياه، وأنظمة توزيع الطاقة في المصانع، وحتى إشارات الطيران والسكك الحديدية. وتكمن الخطورة في أن اختراق نظام تحكّم صناعي (ICS) أو بيئة تحكّم إشرافي وتحصيل البيانات (SCADA) يمكن أن يؤدي إلى عواقب جسيمة تتجاوز الخسائر الإلكترونية، مثل التسبب في انقطاع واسع للطاقة أو تلويث للمياه أو تعطيل لمحطات ضخ النفط. تنبع المشكلة أحياناً من اعتماد هذه الأنظمة على بروتوكولات قديمة لم تصمّم أساساً للعمل عبر الإنترنت، ولكن جرى توصيلها به لاحقاً لأغراض التحديث أو المراقبة عن بُعد. هذا يخلق فجوات أمنية يستغلها المهاجمون للدخول إلى أنظمة حسّاسة كانت في الماضي معزولة تماماً. وفي ظل ازدياد وتيرة "رقمنة" العمليات الصناعية، يتوقع الخبراء أن تصبح استهدافات البنى التحتية ساحة رئيسة للمواجهات السيبرانية في أي نزاع عالمي أو إقليمي مستقبلاً. (Dohi, 2024)

لم يعد الأمن السيبراني مقتصرًا على تأمين دوائر المؤسسة الداخلية، فالاختراق الحديث قد يبدأ من مورد صغير يقدم مكوّنًا برمجياً أو قطعة عتاد يُستخدم داخل الشركة الكبرى. (Abu Alead & Ab) (Altalibe, 2023)

يعرّف هذا النهج بـ"هجوم سلسلة التوريد (Supply Chain Attack)"، حيث يتسلل المخترق إلى برامج التحديث أو المستودعات البرمجية الخاصة بمورد معتمد، ثم يوقع ببرمجيات خبيثة تبدو رسمية تماماً عند تثبيتها. وحين تُثق الشركة الكبرى بتلك التحديثات، تنتقل العدوى إلى أنظمتها تلقائياً قبل أن ينتبه فريق الأمن لأي انحراف. وقد أظهرت وقائع شهيرة مثل حادثة SolarWinds مدى خطورة اختراق الموردين على الأمن القومي لبلادٍ بأكملها، إذ إن البرمجية المخترقة وصلت لأنظمة حسّاسة في العديد من الوكالات والوزارات. (Al-Muadat, Bani Ahmed & Al-Durgham, 2023)

ولتفادي ذلك، باتت كثير من المؤسسات تفرض معايير صارمة لمراقبة سلامة تحديثات البرامج وتشترط تدقيقاً أمنياً متكاملاً لجميع شركاء التوريد. (Al-Tamimi & Mughaid, 2024)

بالرغم من التعقيد التقني المتصاعد للهجمات السيبرانية، ما زال العامل البشري محورياً في نجاح الكثير من الاختراقات. (Al-Quraan & Obaidat, 2023)

تُستغل نقاط الضعف البشرية عبر أساليب الهندسة الاجتماعية، كإرسال رسالة بريد إلكتروني تبدو وكأنها جاءت من رئيس الشركة تطلب بيانات سرية أو تحولاً مالياً "عاجلاً". وغالباً ما يلجأ المهاجمون إلى دراسة دقيقة لتفاصيل الضحية عبر حساباته على الشبكات الاجتماعية، خصوصاً إذا كان الهدف شخصاً ذا صلاحيات واسعة. وحين يُقدّم المخترق نفسه بوصفه ممثلاً للدعم التقني أو أحد عملاء الشركة بعبارات ودّية، قد يصبح ضحية الاحتيال أكثر ميلاً للموافقة على الطلب. ولعل هذا ما يجعل التوعية مكثّفة أمراً لا غنى عنه، إضافةً إلى تطبيق مبادئ المصادقة متعددة العوامل (2FA) وإدارة الصلاحيات بدقة بحيث لا يملك أي موظف منفرداً صلاحيات شاسعة. (Albalushi, Ali & Aman, 2022)

من الهجمات التقليدية التي لا تزال تشكّل كابوساً لكثير من الشركات هجمات الحرمان من الخدمة الموزعة (DDoS)، حيث يجري إغراق خوادم الضحية بحركة مرور وهمية ضخمة تعيق قدرتها على الاستجابة للمستخدمين الفعليين. (Ahmed, Kazar & Harous, 2024)

الجديد في هذا المجال هو سهولة إنشاء شبكات روبوتية (Botnets) تعتمد على أجهزة إنترنت الأشياء ككاميرات المراقبة وأجهزة التوجيه المنزلية، بسبب ضعف إعداداتها الأمنية. فيستغل القراصنة آلاف الأجهزة لاجتياح موقع إلكتروني أو سيرفر حيوي بكميات هائلة من الطلبات خلال ثوانٍ معدودة، ما يضطر الخادم إلى التوقف أو الإبطاء الشديد. ويستخدم البعض هذه الأساليب وسيلةً للابتزاز: "ادفع مبلغاً محدداً وإلا سننفذ هجوماً يُغلق موقعك ويشوه سمعتك." لذا تضطر الشركات لتوظيف شبكات توزيع المحتوى (CDN) وخدمات متخصصة في صدّ هذه الهجمات عبر توزيع الحمل وتصفية الحركة غير الشرعية قبل وصولها للخادم المركزي . (Bouziane & Latreche, 2025)

يستعين عدد متزايد من المؤسسات بالبنى التحتية السحابية بوصفها حلاً لتلبية احتياجاتهم من التخزين والمعالجة أينما وجدوا، لكن ذلك يضيف بُعداً جديداً من المخاطر. (Laib, 2021)

فالسحابات الضخمة تحوي كمّاً هائلاً من البيانات لعملاء متنوعين، وأي ثغرة في إدارة صلاحيات الوصول أو في منظومة التحكم قد تفسح المجال أمام مهاجم للتنقل "أفقياً" بين أنظمة لا تربطها علاقة مباشرة. كما أن التكوين السريع للخوادم الافتراضية (Containers) وإزالة بعضها قد يولّد ثغرات في حال نسيان إغلاق المنفذ أو إزالة كلمة مرور قديمة. يُضاف إلى هذا القلق أن المستخدم قد لا يتحكم تماماً في الطبقات التحتية المادية التي يديرها مزوّد الخدمات السحابية، مما يجعل عملية التدقيق الأمني معقّدة. (Metwally, Abdelazim & Almarji, 2022)

ومع ذلك، عمدت معظم الشركات السحابية الكبيرة إلى تدعيم بيئاتها بوسائل تشفير للبيانات في حالة الراحة وفي أثناء النقل، إضافةً إلى أنظمة تدقيق تلقائي تستشعر أي سلوك خطر يُخالف الأنماط المعتادة. (Badran, Abdel Gaber & Haggag, 2024)

لا يخفى على كثير من المحللين أن بعض الدول تستثمر ميزانيات ضخمة في تطوير "أسلحة سيبرانية" تستخدم إما للهجوم على خصوم محتملين أو كإجراءات ردع تتجاوز النطاق التقليدي للحروب. وفي عالم تكثر فيه التوترات الجيوسياسية، يُصبح اختراق بنى تحتية حيوية—أو التهديد بذلك—وسيلة ضغط سياسية. يحمل هذا السيناريو خطراً مقلقاً يتمثل في انزلاق أي حادثة اختراق إلى صراع دولي علني ما

لم تُضبط الأمور عبر أعراف دبلوماسية وأطر تنسيقية. ولعل تعدد الروايات حول مصدر الهجمات يصعب أحياناً تحديد المسؤولية والمسار القانوني للرد. (Salim & Khammas, 2023)

هنا تبرز الحاجة الملحة لبروتوكولات ردع رقيقي شبيهة بالمعاهدات العسكرية التي تنظم استخدام الأسلحة النووية أو الكيماوية، بحيث تسعى لمنع تصاعد الأعمال العدائية في الفضاء السيبراني.

الفصل الثالث: منهجية وإجراءات الدراسة

1.3 مقدمة

يتناول هذا الفصل الدراسة الميدانية وذلك من خلال التعرف على منهجية الدراسة ومجتمع وعينة الدراسة وأداة الدراسة ومصادر جمع البيانات والأساليب الإحصائية المستخدمة في الدراسة وحساب الصدق والثبات لأداة الدراسة

2.3 منهجية البحث:

يستند البحث على منهجاً وصفيّاً تحليلياً، حيث يركز على فحص الأسس النظرية المتعلقة بالموضوع من خلال استعراض المراجع العربية والأجنبية ذات الصلة. ويتضمن البحث أيضاً تنفيذ دراسة ميدانية تتمثل في توزيع استبيانات على فئات مختلفة من العينة المختارة.

3.3 مجتمع وعينة الدراسة

تمثل مجتمع الدراسة في العاملين في قسم إدارة الأزمات بوزارة الصحة دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية وقامت الدراسة باستخدام أسلوب العينات العشوائية البسيطة لجمع بيانات الدراسة وذلك عن طريق أداة الدراسة المتمثلة في استمارة الاستبيان وقد بلغ عدد أفراد عينة الدراسة 350 فرد وهم الذين أجابوا على استمارة الاستبيان.

4.3 مصادر جمع البيانات والمعلومات:

تعتمد الدراسة على مصدرين أساسيين في جمع البيانات والمعلومات كما يلي:

■ المصادر الثانوية: وتتمثل في الكتب والمراجع العربية والأجنبية ذات الصلة بموضوع الدراسة بالإضافة

إلى الاعتماد على الأبحاث والدراسات السابقة والدوريات والمجلات العلمية والمقالات

- المصادر الأولية: حيث تعتمد الدراسة على الاستبانة كأداة رئيسية في جمع البيانات من مصادرها والتي تم تصميمها خصيصاً لهذا الغرض على Google Forms وإرسال رابطها إلى مجتمع الدراسة

5.3 الأساليب الإحصائية:

قام البحث باستخدام البرنامج الإحصائي SPSS لتحليل بيانات الدراسة باستخدام مجموعة من الأساليب الإحصائية كما يلي:

- معامل الفاكورنباخ لحساب مستوي ثبات أداة الدراسة
- معامل ارتباط بيرسون لتحديد مستوي الاتساق الداخلي وصدق أداة الدراسة وللتعرف على العلاقة بين متغيرات الدراسة
- النسب والتكرارات لوصف خصائص عينة الدراسة
- الوسط الحسابي والانحراف المعياري لوصف مستوي استجابة افراد عينة الدراسة لعبارات أداة الدراسة
- معادلة الانحدار الخطي البسيط لقياس الأثر بين متغيرات الدراسة

6.3 أداة الدراسة

تم العمل على الاستبانة للتناسب مع متغيرات الدراسة من خلال الاطلاع على الدراسات السابقة المتعلقة بموضوع الدراسة، حيث تكونت من قسمين رئيسيين هما:

- القسم الأول: وهو الجزء الخاص بالمتغيرات الديمغرافية لأفراد عينة الدراسة، والمتمثلة بـ: النوع الاجتماعي، والعمر، والمؤهل العلمي، والوضع المهني،
- القسم الثاني: اشتمل القسم الثاني على الفقرات والأبعاد التي تقيس متغيرات الدراسة المستقل والتابع. وتضمنت العبارات المتعلقة بالمتغير المستقل (إدارة مخاطر العامل البشري) وتضمن ثلاث ابعاد (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) واشتملت على 15

عبارات والعبارات المتعلقة بالمتغير التابع (الحد من الهجمات السيبرانية) دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية واشتملت على 10 عبارة وتم استخدام مقياس ليكرت ذو الخمس درجات الذي يتكون من موافق جدا (5)، موافق (4)، محايد (3)، غير موافق (2)، غير موافق جدا (1) في الإجابة على أسئلة محاور الدراسة.

وقد قامت الدراسة بتقسيم اتجاه موافقة أفراد عينة الدراسة على عبارات محاور الدراسة إلى مستويات من خلال تطبيق ما يلي:

- مدي المقياس = أعلي رقم في المقياس (5) – أقل رقم في المقياس (1) = 4
- مدي المستوي = مدي المقياس / عدد المستويات (5) = 0.80

جدول (1) مستويات موافقة عينة الدراسة على عبارات أداة الدراسة

الدرجة	المستوي
1.79 – 1	منخفضة جدا
2.59 – 1.80	منخفضة
3.39 – 2.60	متوسطة
4.19 – 3.40	مرتفعة
5.00 – 4.20	مرتفعة جدا

7.3 صدق أداة الدراسة

تم حساب صدق عبارات استمارة الاستبيان عن طريق تحديد مستوي التجانس الداخلي من خلال التعرف على الدلالة الإحصائية لمعاملات الارتباط بيرسون بين درجة العبارة والدرجة الكلية للمحور الذي تنتهي إليه العبارة وجاءت النتائج كما يلي:

☑ المحور الأول: إدارة مخاطر العامل البشري

جدول (2) معاملات الارتباط لعبارات المحور الاول

م	العبارة	معامل ارتباط بيرسون	Sig
تحديد وتقييم المخاطر			
1	تقوم المؤسسة بتحديد المخاطر البشرية المحتملة التي قد تؤثر على أمن المعلومات.	0.588**	0.000
2	يتم تقييم تأثير العامل البشري ضمن تحليل شامل لمصادر التهديد السيبراني.	0.687**	0.000
3	تُستخدم أدوات تقييم مهنية لرصد السلوكيات البشرية التي قد تؤدي إلى اختراقات أمنية.	0.481**	0.000
4	تعتمد المؤسسة على بيانات سابقة لتحليل الحوادث المرتبطة بالعامل البشري.	0.607**	0.000
5	يتم تضمين الموظفين في عمليات تحديد المخاطر المتعلقة بالأمن السيبراني.	0.646**	0.000
معالجة إدارة المخاطر			
6	توفر المؤسسة برامج تدريبية متخصصة للتقليل من أخطاء العامل البشري.	0.778**	0.000
7	توجد سياسات واضحة للتعامل مع السلوكيات التي تهدد أمن المعلومات.	0.590**	0.000
8	يتم تطوير خطط عمل لمعالجة الثغرات التي يسببها العامل البشري.	0.782**	0.000
9	تعتمد المؤسسة حلولاً تقنية تقلل من احتمالية حدوث الخطأ البشري.	0.795**	0.000

م	العبارة	معامل ارتباط بيرسون	Sig
10	تُشرك إدارة الموارد البشرية في خطط تقليل المخاطر السيبرانية الناتجة عن الموظفين.	0.488**	0.000
مراقبة إدارة المخاطر			
11	تراقب المؤسسة بشكل دوري سلوك الموظفين المتعلق باستخدام الأنظمة الإلكترونية.	0.721**	0.000
12	توجد آليات إنذار مبكر لاكتشاف أي نشاط غير معتاد ناتج عن العنصر البشري.	0.730**	0.000
13	يتم تحديث إجراءات المراقبة بشكل دوري لمواكبة تطور التهديدات البشرية.	0.529**	0.000
14	يتم توثيق ومراجعة حوادث الاختراق الناتجة عن العامل البشري بشكل منتظم.	0.634**	0.000
15	يتم إعداد تقارير دورية حول التزام الموظفين بسياسات الأمن السيبراني.	0.671**	0.000

** ذات دلالة إحصائية عند 0.01

وتبين أن جميع معاملات الارتباط لجميع عبارات محور إدارة مخاطر العامل البشري كانت ذات دلالة إحصائية عند مستوى معنوية (0.01) وهذا يعني أن عبارات محور إدارة مخاطر العامل البشري تتمتع بصدق الاتساق الداخلي وهي صالحة لأغراض الدراسة.

☒ المحور الثاني: الحد من الهجمات السيبرانية

جدول (3) معاملات الارتباط لعبارات المحور الثاني

م	العبارة	معامل ارتباط بيرسون	Sig
1	تمتلك المؤسسة خطة استجابة واضحة للهجمات السيبرانية.	0.694**	0.000
2	تُحدَّث أنظمة الحماية بشكل مستمر لتقليل احتمالية الهجمات.	0.709**	0.000
3	تعتمد المؤسسة على أدوات متقدمة لرصد التهديدات السيبرانية.	0.649**	0.000
4	يتم اختبار أنظمة الأمن السيبراني بانتظام للتأكد من كفاءتها.	0.725**	0.000
5	يتم التعامل مع أي محاولة اختراق بسرعة وفعالية.	0.652**	0.000
6	توجد آليات تحقق متعددة الهوية (MFA) لحماية الأنظمة.	0.750**	0.000
7	تُجرى محاكاة دورية لهجمات سيبرانية للتدريب على مواجهتها.	0.448**	0.000
8	تُستخدم حلول تشفير قوية لحماية البيانات الحساسة.	0.649**	0.000
9	يتم تقييم المخاطر السيبرانية الجديدة عند كل تحديث للنظام.	0.630**	0.000
10	تعتمد المؤسسة إجراءات صارمة للحد من وصول غير المصرح به إلى المعلومات.	0.673**	0.000

** ذات دلالة احصائية عند 0.01

وتبين أن جميع معاملات الارتباط لجميع عبارات محور الحد من الهجمات السيبرانية كانت ذات دلالة إحصائية عند مستوى معنوية (0.01) وهذا يعني أن عبارات محور الحد من الهجمات السيبرانية تتمتع بصدق الاتساق الداخلي وهي صالحة لأغراض الدراسة.

8.3 ثبات أداة الدراسة:

تم حساب معامل ألفا كرونباخ لعبارات محاور الاستبيان وكانت النتائج كما يلي:

جدول (4) معامل الثبات لمحاور استمارة الاستبيان

المحاور	معامل الفا كرونباخ	عدد العبارات
إدارة مخاطر العامل البشري	0.850	20
الحد من الهجمات السيبرانية	0.898	10
إجمالي استمارة الاستبيان	0.929	30

يتبين أن قيمة معامل الثبات Alpha أكبر من 0.7 لجميع محاور استمارة الاستبيان مما يؤكد على

صلاحية وارتباط عبارات محاور استمارة الاستبيان وارتفاع مستوى ثبات أداة الدراسة مما يسمح

باستخدام الأداة لغرض الدراسة.

الفصل الرابع: تحليل النتائج

1.4 مقدمة

سوف نتناول في هذا الفصل تحليل بيانات الدراسة من خلال تحليل استمارة الاستبيان والتعرف على خصائص عينة الدراسة وتحليل محاور الدراسة واختبار فروض الدراسة من أجل تحقيق أهداف الدراسة والوصول إلى نتائج وتوصيات للدراسة.

2.4 خصائص عينة الدراسة

جدول (5) توزيع عينة الدراسة وفقا لخصائصها

الخاصية	الفئات	العدد	%
النوع الاجتماعي	ذكر	250	71.4
	أنثى	100	28.5
العمر	أقل من 25 سنة	60	17.1
	من 25 الى أقل من 35 سنة	100	28.5
	من 35 الى أقل من 45 سنة	100	28.5
	45 سنة فأكثر	90	25.7
المؤهل العلمي	ثانوي	90	25.7
	بكالوريوس	130	37.1
	ماجستير	100	28.5
	دكتوراه	30	8.5
الوضع المهني	مدير	150	42.8
	نائب مدير	120	34.2
	رئيس قسم	80	22.8

3.4 تحليل استمارة الاستبيان

✓ المحور الأول: إدارة مخاطر العامل البشري

1- تحديد وتقييم المخاطر

جدول (6) المتوسط الحسابي والانحراف المعياري والترتيب ومستوي الموافقة على عبارات تحديد

وتقييم المخاطر

العبارة	المتوسط الحسابي	الانحراف المعياري	الترتيب	مستوي الموافقة
تقوم المؤسسة بتحديد المخاطر البشرية المحتملة التي قد تؤثر على أمن المعلومات.	4.253	0.683	4	مرتفع جدا
يتم تقييم تأثير العامل البشري ضمن تحليل شامل لمصادر التهديد السيبراني.	4.276	0.766	2	مرتفع جدا
تُستخدم أدوات تقييم مهنية لرصد السلوكيات البشرية التي قد تؤدي إلى اختراقات أمنية.	4.198	0.773	5	مرتفع
تعتمد المؤسسة على بيانات سابقة لتحليل الحوادث المرتبطة بالعامل البشري.	4.372	0.564	1	مرتفع جدا
يتم تضمين الموظفين في عمليات تحديد المخاطر المتعلقة بالأمن السيبراني.	4.273	0.775	3	مرتفع جدا
المتوسط	4.274	0.712		مرتفع

تم ترتيب عبارات تحديد وتقييم المخاطر من حيث درجة الأهمية النسبية (قيمة المتوسط

الحسابي الأكبر) من وجهة نظر عينة الدراسة تبين أن عبارة (تعتمد المؤسسة على بيانات سابقة لتحليل

الحوادث المرتبطة بالعامل البشري) هي أكثر العبارات أهمية بقيمة 4.372 وانحراف معياري 0.564 وبدرجة موافقة مرتفعة جداً بينما كانت العبارة (تُستخدم أدوات تقييم مهنية لرصد السلوكيات البشرية التي قد تؤدي إلى اختراقات أمنية) هي أقل العبارات أهمية بقيمة 4.198 وانحراف معياري 0.773 وبدرجة موافقة مرتفعة وعند دراسة عبارات تحديد وتقييم المخاطر تبين أن أربع عبارات في مستوى الموافقة المرتفع جداً وعبارة واحدة في مستوى الموافقة المرتفع مما يوضح وجود مستوى مرتفع جداً من تحديد وتقييم المخاطر كأحد ابعاد إدارة مخاطر العامل البشري حيث بلغت قيمة المتوسط الحسابي 4.274 بانحراف معياري 0.712

2- معالجة إدارة المخاطر

جدول (7) المتوسط الحسابي والانحراف المعياري والترتيب ومستوى الموافقة على عبارات معالجة

إدارة المخاطر

العبارة	المتوسط الحسابي	الانحراف المعياري	الترتيب	مستوى الموافقة
توفر المؤسسة برامج تدريبية متخصصة للتقليل من أخطاء العامل البشري.	4.359	0.709	2	مرتفع جداً
توجد سياسات واضحة للتعامل مع السلوكيات التي تهدد أمن المعلومات.	4.161	0.758	5	مرتفع
يتم تطوير خطط عمل لمعالجة الثغرات التي يسببها العامل البشري.	4.253	0.659	4	مرتفع جداً
تعتمد المؤسسة حلولاً تقنية تقلل من احتمالية حدوث الخطأ البشري.	4.396	0.634	1	مرتفع جداً
تُشرك إدارة الموارد البشرية في خطط تقليل المخاطر السيبرانية الناتجة عن الموظفين.	4.315	0.615	3	مرتفع جداً
المتوسط	4.297	0.675		مرتفع جداً

تم ترتيب عبارات معالجة إدارة المخاطر من حيث درجة الأهمية النسبية (قيمة المتوسط الحسابي الأكبر) من وجهة نظر عينة الدراسة تبين أن عبارة (تعتمد المؤسسة حلولاً تقنية تقلل من احتمالية حدوث الخطأ البشري) هي أكثر العبارات أهمية بقيمة 4.396 وانحراف معياري 0.634 وبدرجة موافقة مرتفعة جداً بينما كانت العبارة (توجد سياسات واضحة للتعامل مع السلوكيات التي تهدد أمن المعلومات) هي أقل العبارات أهمية بقيمة 4.161 وانحراف معياري 0.758 وبدرجة موافقة مرتفعة وعند دراسة عبارات معالجة إدارة المخاطر تبين أن أربع عبارات في مستوى الموافقة المرتفع جداً وعبارة واحدة في مستوى الموافقة المرتفع مما يوضح وجود مستوى مرتفع جداً من معالجة إدارة المخاطر كأحد أبعاد إدارة مخاطر العامل البشري حيث بلغت قيمة المتوسط الحسابي 4.297 وانحراف معياري 0.675

3- مراقبة إدارة المخاطر

جدول (8) المتوسط الحسابي والانحراف المعياري والترتيب ومستوى الموافقة على عبارات مراقبة

إدارة المخاطر

العبارة	المتوسط الحسابي	الانحراف المعياري	الترتيب	مستوى الموافقة
تراقب المؤسسة بشكل دوري سلوك الموظفين المتعلق باستخدام الأنظمة الإلكترونية.	4.375	0.564	3	مرتفع جداً
توجد آليات إنذار مبكر لاكتشاف أي نشاط غير معتاد ناتج عن العنصر البشري.	4.453	0.539	1	مرتفع جداً
يتم تحديث إجراءات المراقبة بشكل دوري لمواكبة تطور التهديدات البشرية.	4.391	0.633	2	مرتفع جداً
يتم توثيق ومراجعة حوادث الاختراق الناتجة عن العامل البشري بشكل منتظم.	4.266	0.731	4	مرتفع جداً

مرتفع جدا	5	0.773	4.216	يتم إعداد تقارير دورية حول التزام الموظفين بسياسات الأمن السيبراني.
مرتفع جدا		0.648	4.340	المتوسط

تم ترتيب عبارات مراقبة إدارة المخاطر من حيث درجة الأهمية النسبية (قيمة المتوسط الحسابي الأكبر) من وجهة نظر عينة الدراسة تبين أن عبارة (توجد آليات إنذار مبكر لاكتشاف أي نشاط غير معتاد ناتج عن العنصر البشري) هي أكثر العبارات أهمية بقيمة 4.453 وانحراف معياري 0.539 وبدرجة موافقة مرتفعة جدا بينما كانت العبارة (يتم إعداد تقارير دورية حول التزام الموظفين بسياسات الأمن السيبراني) هي أقل العبارات أهمية بقيمة 4.216 وانحراف معياري 0.773 وبدرجة موافقة مرتفعة وعند دراسة عبارات مراقبة إدارة المخاطر تبين أن جميع العبارات في مستوى الموافقة المرتفع جدا مما يوضح وجود مستوى مرتفع جدا من مراقبة إدارة المخاطر كأحد ابعاد إدارة مخاطر العامل البشري حيث بلغت قيمة المتوسط الحسابي 4.340 بانحراف معياري 0.648

☑ المحور الثاني: الحد من الهجمات السيبرانية

جدول (9) المتوسط الحسابي والانحراف المعياري والترتيب ومستوى الموافقة على عبارات الحد من

الهجمات السيبرانية

العبرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	مستوى الموافقة
تمتلك المؤسسة خطة استجابة واضحة للهجمات السيبرانية.	4.169	0.953	3	مرتفع
تُحدَّث أنظمة الحماية بشكل مستمر لتقليل احتمالية الهجمات.	4.076	0.796	7	مرتفع

العبارة	المتوسط الحسابي	الانحراف المعياري	الترتيب	مستوي الموافقة
تعتمد المؤسسة على أدوات متقدمة لرصد التهديدات السيبرانية.	4.091	0.855	5	مرتفع
يتم اختبار أنظمة الأمن السيبراني بانتظام للتأكد من كفاءتها.	4.154	0.678	4	مرتفع
يتم التعامل مع أي محاولة اختراق بسرعة وفعالية.	4.010	0.754	8	مرتفع
توجد آليات تحقق متعددة الهوية (MFA) لحماية الأنظمة.	3.982	0.780	9	مرتفع
تُجرى محاكاة دورية لهجمات سيبرانية للتدريب على مواجهتها.	4.078	0.764	6	مرتفع
تُستخدم حلول تشفير قوية لحماية البيانات الحساسة.	3.917	0.907	10	مرتفع
يتم تقييم المخاطر السيبرانية الجديدة عند كل تحديث للنظام.	4.221	0.667	2	مرتفع جدا
تعتمد المؤسسة إجراءات صارمة للحد من وصول غير المصرح به إلى المعلومات.	4.250	0.596	1	مرتفع جدا
المتوسط	4.095	0.775		مرتفع

تم ترتيب عبارات الحد من الهجمات السيبرانية من حيث درجة الأهمية النسبية (قيمة المتوسط الحسابي الأكبر) من وجهة نظر عينة الدراسة تبين أن عبارة (تعتمد المؤسسة إجراءات صارمة للحد من وصول غير المصرح به إلى المعلومات) هي أكثر العبارات أهمية بقيمة 4.250 وانحراف معياري 0.596 وبدرجة موافقة مرتفعة جدا بينما كانت العبارة (تُستخدم حلول تشفير قوية لحماية البيانات الحساسة) هي أقل

العبارات اهمية بقيمة 3.917 وانحراف معياري 0.907 وبدرجة موافقة مرتفعة وعند دراسة عبارات الحد من الهجمات السيبرانية تبين أن عبارتين في مستوى الموافقة المرتفع جدا وثمانية عبارات في مستوى الموافقة المرتفع مما يوضح ارتفاع مستوى الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية المحدودة حيث بلغت قيمة المتوسط الحسابي 4.095 بانحراف معياري 0.775.

3.4 اختبارفروض الدراسة

❖ الفرضية الرئيسية: لا يوجد أثر ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) لإدارة مخاطر العامل البشري بأبعادها (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية

جدول (10) نتائج نموذج الانحدار الخطي البسيط لأثر إدارة مخاطر العامل البشري على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية

P-VALUE	R	R ²	F	T	B
0.000	0.769	0.592	**553.350	**23.523	0.992

المصدر: نتائج التحليل الإحصائي ببرنامج SPSS 23

** ذات دلالة احصائية عند 0.01

يتبين من الجدول (10) وجود أثر طردي ذي دلالة إحصائية لمستوى إدارة مخاطر العامل البشري بأبعادها (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى 0.05 حيث كانت قيمة (Sig F) = 0.000 وهي قيمة أقل من 0.05 أي أن قيمة F المحسوبة أكبر من قيمة F الجدولية واتضح وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية بين إدارة مخاطر العامل البشري بأبعادها (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى معنوية 0.05 واتضح

ان المتغير المستقل (إدارة مخاطر العامل البشري) يفسر 76.9 % من التغيرات التي تحدث في المتغير التابع (الحد من الهجمات السيبرانية) وان باقي التغيرات ترجع لمتغيرات اخرى لم تدخل في النموذج وتبين أن كلما ازداد مستوى إدارة مخاطر العامل البشري بمقدار 1 % ازداد مستوى إدارة مخاطر العامل البشري بأبعادها (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية بمقدار 0.446% مما يبين عدم صحة الفرضية الرئيسية للدراسة.

❖ **الفرضية الفرعية الاولى:** لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha 0.005$) لتحديد وتقييم المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية ، مع الدور الوسيط لالتزام المنظمة بتطبيق معايير السلامة.

جدول (11) نتائج نموذج الانحدار الخطي البسيط لأثر تحديد وتقييم المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية

P-VALUE	R	R ²	F	T	B
0.000	0.746	0.557	**480.129	**21.912	0.361

المصدر: نتائج التحليل الإحصائي ببرنامج SPSS 23

** ذات دلالة احصائية عند 0.01

يتبين من الجدول (11) وجود أثر طردي ذي دلالة إحصائية لمستوى تحديد وتقييم المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى 0.05 حيث كانت قيمة (Sig F) = 0.000 وهي قيمة أقل من 0.05 أي أن قيمة F المحسوبة أكبر من قيمة F الجدولية واتضح وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية بين تحديد وتقييم المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى معنوية 0.05 واتضح ان المتغير المستقل (تحديد وتقييم المخاطر) يفسر 55.7 % من التغيرات التي تحدث في المتغير التابع (الحد من الهجمات السيبرانية) وان باقي التغيرات ترجع لمتغيرات اخرى لم تدخل

في النموذج وتبين أن كلما ازداد مستوى تحديد وتقييم المخاطر بمقدار 1 % ازداد مستوى للتخطيط الاستراتيجي على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية بمقدار 0.361% مما يبين عدم صحة الفرضية الفرعية الاولى للدراسة.

❖ الفرضية الفرعية الثانية: لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية (≥ 0.005)

لمعالجة إدارة المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية من خلال الدور الوسيط لتوفير المعدات والوسائل الوقائية.

جدول (12) نتائج نموذج الانحدار الخطي البسيط لأثر معالجة إدارة المخاطر على الحد من الهجمات

السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية

P-VALUE	R	R ²	F	T	B
0.000	0.694	0.481	**354.427	**18.826	0.337

المصدر: نتائج التحليل الإحصائي ببرنامج SPSS 23

** ذات دلالة احصائية عند 0.01

يتبين من الجدول (12) وجود أثر طردي ذي دلالة إحصائية لمستوى معالجة إدارة المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى 0.05 حيث كانت قيمة (Sig F) = 0.000 وهي قيمة أقل من 0.05 أي أن قيمة F المحسوبة أكبر من قيمة F الجدولية واتضح وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية بين معالجة إدارة المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى معنوية 0.05 واتضح ان المتغير المستقل (معالجة إدارة المخاطر) يفسر 48.1 % من التغيرات التي تحدث في المتغير التابع (الحد من الهجمات السيبرانية) وان باقي التغيرات ترجع لمتغيرات اخرى لم تدخل في النموذج وتبين أن كلما ازداد مستوى معالجة إدارة المخاطر بمقدار 1 % ازدادت الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية بمقدار 0.337 % مما يبين عدم صحة الفرضية الفرعية الثانية للدراسة.

❖ الفرضية الفرعية الثالثة: لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \geq 0.005$) لمراقبة

إدارة المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة

العربية السعودية ، مع اختبار الدور الوسيط للإبلاغ والاستجابة للحوادث المهنية

جدول (13) نتائج نموذج الانحدار الخطي البسيط لأثر مراقبة إدارة المخاطر على الحد من الهجمات

السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية

P-VALUE	R	R ²	F	T	B
0.000	0.650	0.422	**279.317	**16.713	0.294

المصدر: نتائج التحليل الإحصائي برنامج SPSS 23

** ذات دلالة احصائية عند 0.01

يتبين من الجدول (13) وجود أثر طردي ذي دلالة إحصائية لمستوى مراقبة إدارة المخاطر على

الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند

مستوى 0.05 حيث كانت قيمة (Sig F) = 0.000 وهي قيمة أقل من 0.05 أي أن قيمة F المحسوبة أكبر من

قيمة F الجدولية واتضح وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية بين مراقبة إدارة المخاطر على

الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند

مستوى معنوية 0.05 واتضح ان المتغير المستقل (مراقبة إدارة المخاطر) يفسر 42.2 % من التغيرات التي

تحدث في المتغير التابع (الحد من الهجمات السيبرانية) وان باقي التغيرات ترجع لمتغيرات اخري لم تدخل في

النموذج وتبين أن كلما ازداد مستوى مراقبة إدارة المخاطر بمقدار 1 % ازداد مستوى الحد من الهجمات

السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية بمقدار 0.294 % مما

يبين عدم صحة الفرضية الفرعية الثالثة للدراسة.

الفصل الخامس: النتائج والتوصيات والمقترحات

1.5 مقدمة

سوف نتناول في هذا الفصل النتائج التي توصلت إليها الدراسة من خلال تحليل البيانات المتعلقة بمحاور الدراسة والتي تم الحصول عليها عن طريق أداة الاستبيان المتمثلة في استمارة الاستبيان واختبار فروض الدراسة من أجل تحقيق أهداف الدراسة وكذلك يتناول الفصل مجموعة من التوصيات التي توصي بها الدراسة ومجموعة من المقترحات لدراسات وابحاث يمكن اجراؤها في المستقبل

2.5 نتائج الدراسة

- ✓ وجود مستوي مرتفع جدا من تحديد وتقييم المخاطر كأحد ابعاد إدارة مخاطر العامل البشري حيث بلغت قيمة المتوسط الحسابي 4.274 بانحراف معياري 0.712
- ✓ وجود مستوي مرتفع جدا من معالجة إدارة المخاطر كأحد ابعاد إدارة مخاطر العامل البشري حيث بلغت قيمة المتوسط الحسابي 4.297 بانحراف معياري 0.675
- ✓ وجود مستوي مرتفع جدا من مراقبة إدارة المخاطر كأحد ابعاد إدارة مخاطر العامل البشري حيث بلغت قيمة المتوسط الحسابي 4.340 بانحراف معياري 0.648
- ✓ وجود مستوي مرتفع جدا من كأحد ابعاد إدارة مخاطر العامل البشري حيث بلغت قيمة المتوسط الحسابي 4.297 بانحراف معياري 0.675
- ✓ ارتفاع مستوى الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية المحدودة حيث بلغت قيمة المتوسط الحسابي 4.095 بانحراف معياري 0.775.
- ✓ وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية بين إدارة مخاطر العامل البشري بأبعادها (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوي معنوية 0.05 واتضح ان المتغير المستقل (إدارة مخاطر العامل البشري) يفسر 76.9 % من التغيرات

التي تحدث في المتغير التابع (الحد من الهجمات السيبرانية) وان باقي التغيرات ترجع لمتغيرات اخري لم تدخل في النموذج وتبين أن كلما ازداد مستوى إدارة مخاطر العامل البشري بمقدار 1 % ازداد مستوى إدارة مخاطر العامل البشري بأبعادها (تحديد وتقييم المخاطر، معالجة إدارة المخاطر، مراقبة إدارة المخاطر) على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية بمقدار 0.446% مما يبين عدم صحة الفرضية الرئيسية للدراسة.

✓ وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية بين تحديد وتقييم المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى معنوية 0.05 واتضح ان المتغير المستقل (تحديد وتقييم المخاطر) يفسر 55.7% من التغيرات التي تحدث في المتغير التابع (الحد من الهجمات السيبرانية) وان باقي التغيرات ترجع لمتغيرات اخري لم تدخل في النموذج وتبين أن كلما ازداد مستوى تحديد وتقييم المخاطر بمقدار 1 % ازداد مستوى للتخطيط الاستراتيجي على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية بمقدار 0.361% مما يبين عدم صحة الفرضية الفرعية الاولى للدراسة.

✓ وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية بين معالجة إدارة المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى معنوية 0.05 واتضح ان المتغير المستقل (معالجة إدارة المخاطر) يفسر 48.1% من التغيرات التي تحدث في المتغير التابع (الحد من الهجمات السيبرانية) وان باقي التغيرات ترجع لمتغيرات اخري لم تدخل في النموذج وتبين أن كلما ازداد مستوى معالجة إدارة المخاطر بمقدار 1 % ازدادت الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية بمقدار 0.337% مما يبين عدم صحة الفرضية الفرعية الثانية للدراسة.

✓ وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية بين مراقبة إدارة المخاطر على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى معنوية 0.05 واتضح ان المتغير المستقل (مراقبة إدارة المخاطر) يفسر 42.2% من التغيرات التي تحدث في المتغير التابع (الحد من الهجمات السيبرانية) وان باقي التغيرات ترجع لمتغيرات اخري لم تدخل في النموذج وتبين أن كلما ازداد مستوى مراقبة إدارة المخاطر بمقدار 1 % ازداد مستوى الحد

من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية بمقدار 0.294 % مما يبين عدم صحة الفرضية الفرعية الثالثة للدراسة.

✓ وجود علاقة ارتباط طردية قوية ذات دلالة إحصائية بين على الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية عند مستوى معنوية 0.05 واتضح ان المتغير المستقل (إدارة مخاطر العامل البشري) يفسر 48.1 % من التغيرات التي تحدث في المتغير التابع (الحد من الهجمات السيبرانية) وان باقي التغيرات ترجع لمتغيرات اخري لم تدخل في النموذج وتبين أن كلما ازداد مستوى بمقدار 1 % ازداد مستوى الحد من الهجمات السيبرانية دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية بمقدار 0.337 % مما يبين عدم صحة الفرضية الفرعية الرابعة للدراسة.

3.5 التوصيات

- ✓ تعزيز برامج التوعية الأمنية المستمرة لجميع الموظفين، مع التركيز على التهديدات السيبرانية المرتبطة بالسلوك البشري كالهندسة الاجتماعية والتصيد الإلكتروني.
- ✓ تضمين إدارة مخاطر العامل البشري ضمن الخطة الاستراتيجية للأمن السيبراني في المؤسسات الحكومية لضمان معالجة التهديدات البشرية بشكل منهجي.
- ✓ تصميم اختبارات تقييم دورية للموظفين لقياس مدى التزامهم وفهمهم للسياسات الأمنية ومعايير حماية المعلومات.
- ✓ تفعيل أنظمة الرقابة والتحقق متعددة المستويات لضمان الكشف المبكر عن الأنشطة غير المصرح بها الناتجة عن خطأ أو سلوك بشري مقصود.
- ✓ دمج وحدات إدارة الموارد البشرية مع إدارات الأمن السيبراني لإيجاد بيئة عمل تدعم السلوك الأمني المسؤول والوقائي.
- ✓ تطبيق سياسة العقوبات والمكافآت لربط الالتزام بالإجراءات الأمنية بمستوى الأداء الوظيفي.

- ✓ تحديث السياسات الأمنية باستمرار لمواكبة التطورات التكنولوجية والتكتيكات الجديدة التي قد تستغل العامل البشري.
- ✓ تطوير سيناريوهات محاكاة للهجمات السيبرانية تتضمن عناصر بشرية لتدريب الموظفين على التصرف السليم في حال التعرض لمحاولات اختراق.
- ✓ إشراك الموظفين في تطوير إجراءات الأمن السيبراني لرفع مستوى الالتزام والإدراك بالمخاطر المحتملة.
- ✓ تعزيز ثقافة العمل الوقائي والتبليغ الفوري عن أي سلوك مشبوه من خلال قنوات رسمية ومؤمنة داخل المؤسسة.

4.5 المقترحات

- إجراء دراسات مقارنة بين القطاعات الحكومية والخاصة في المملكة لقياس الفروقات في مستوى إدارة مخاطر العامل البشري.
- توسيع الدراسة لتشمل الأقاليم الإدارية المختلفة في المملكة لرصد التباين الجغرافي في الاستجابة للمخاطر البشرية السيبرانية.
- اقتراح إنشاء وحدة مستقلة لإدارة مخاطر السلوك البشري في كل مؤسسة حكومية مرتبطة بوحدة الأمن السيبراني.
- تصميم منصة وطنية موحدة للتدريب على الأمن السيبراني موجهة لموظفي القطاع العام مع تركيز خاص على أخطاء العامل البشري.
- دراسة أثر التحفيز المالي والمعنوي على مدى التزام الموظفين بالسلوكيات الأمنية الصحيحة.
- البحث في العلاقة بين مستوى التعليم والتخصص الوظيفي ومدى الوعي بالمخاطر السيبرانية لدى الموظفين الحكوميين.
- اقتراح إطار وطني لإدارة مخاطر العامل البشري يعزز منسوب الحوكمة الإلكترونية على مستوى القطاع العام.

- إجراء دراسات طولية لقياس تطور تأثير البرامج التدريبية على سلوك الموظفين في مجال الأمن السيبراني.
- تحليل أسباب ضعف الالتزام بالإجراءات الأمنية من منظور نفسي واجتماعي وليس فقط من الناحية التقنية.
- دراسة أثر ثقافة المؤسسة التنظيمية على مدى فعاليتها في منع الأخطاء البشرية المرتبطة بالهجمات السيبرانية.

Abstract

The study aims to determine the impact of applying human factor risk management, with its combined dimensions (risk identification and assessment, risk management treatment, and risk management monitoring), on reducing cyberattacks: a field study on government institutions in the Kingdom of Saudi Arabia. The descriptive-analytical approach was adopted, and a questionnaire was distributed to a random sample of employees in government banks in Riyadh. The number of valid questionnaires for analysis was 350. The researcher used a set of statistical methods to analyze the data.

The study results showed a very high level of risk identification and assessment as one of the dimensions of human factor risk management, as well as a very high level of risk management treatment.

In light of the findings, the study recommends enhancing ongoing security awareness programs for all employees, with a focus on cyber threats related to human behavior such as social engineering and phishing. It also recommends incorporating human factor risk management into the strategic cybersecurity plan of government institutions to ensure systematic handling of human-related threats.

Keywords: Human Factor Risks – Cyberattacks – Government Institutions

قائمة المراجع

أولاً: المراجع باللغة العربية

1. أبو نصرة، أشرف أحمد محمد، الكايد، وائل جمال عبدالكريم، و الرقاد، محمد عبدالكريم سالم. (2020). أثر التخطيط الاستراتيجي في إدارة المخاطر في البنوك التجارية الأردنية (رسالة ماجستير غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
2. باقر، وفاء جاسم علي عباس، ارتيمة، هاني جزاع عبدالكريم، و الهواري، سامر فواز. (2020). أثر إدارة المخاطر في إدارة المشاريع الهندسية: الدور الوسيط للثقافة المنظمة في الهيئة العامة للطرق والنقل البري في دولة الكويت (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
3. بني مصطفى، عبيدة محمد حسين، و العفيف، جمال حسن عيسى. (2022). أثر فاعلية نظم المعلومات المحاسبية في إدارة المخاطر المؤسسية: دراسة ميدانية على المصارف الإسلامية الأردنية (رسالة ماجستير غير منشورة). جامعة جرش، جرش.
4. الجمل، أسيل كمال ربيعي، و العيطان، غيث ناصر محمد. (2023). أثر إدارة المخاطر على الأداء المالي للبنوك التجارية الأردنية (رسالة ماجستير غير منشورة). جامعة آل البيت، المفرق.
5. الحسيني، عبدالله بن حمود بن محمد، و الخشالي، شاكِر جار الله محمود. (2022). أثر التفكير الاستراتيجي في إدارة المخاطر: الدور المعدل للدعم المنظمي في شركات المقاولات العمانية (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
6. حفصي، أسماء، بن منصور، ملاك، و بن محمود، الحاج عرابة. (2022). أثر مخاطر إدارة الإمداد في المؤسسة في ظل جائحة كورونا: دراسة حالة شركة الطاسيلي للخدمات البترولية - منطقة إرارة 2 - حاسي مسعود (رسالة ماجستير غير منشورة). جامعة قاصدي مرباح - ورقلة، ورقلة.
7. الرواشدة، عبدالله محمد عبدالله، و الهلسة، رولى هاني سلمان. (2022). أثر ريادة الأعمال على إدارة المخاطر للمشاريع وفق نظام COSO (رسالة ماجستير غير منشورة). جامعة مؤتة، مؤتة.

8. الرواشدة، ينال عاطف سلام، و الشورة، عبدالله أحمد سليمان. (2022). أثر إدارة المخاطر في مرونة سلسلة التوريد: الدور المعدل للتمكين في شركة البوتاس العربية (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
9. زين، ياسمين إلياس عطا، و الشاعر، سوسن عبدالله حمد الله. (2023). أثر التجديد الاستراتيجي في إدارة المخاطر في شركات التأمين الأردنية (رسالة ماجستير غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
10. سلمونة، محمد ياسين محمد، و هماش، عبدالسلام أحمد إسماعيل. (2024). المسؤولية الدولية الناشئة عن الهجمات السيبرانية (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
11. الشوحة، ريم عبدالله فلاح، و الحياصات، حمدان محمد. (2020). أثر فاعلية التدقيق الداخلي في إدارة المخاطر المؤسسية: الدور الوسيط لنظم تخطيط موارد المنشأة (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
12. الصمادي، دعاء حسين أحمد، و الرواشدة، هاني علي عارف. (2023). أثر خصائص مجلس الإدارة على الإفصاح عن المخاطر المالية: الدور المعدل لجودة التدقيق الخارجي: دراسة تطبيقية على شركات الصناعية المدرجة في بورصة عمان (رسالة ماجستير غير منشورة). جامعة جرش، جرش.
13. العليمات، عبير عبدالله سليمان، و الشيخ، عماد يوسف أحمد أحمد. (2023). أثر إدارة المخاطر المؤسسية وفقاً لإطار "COSO" في الأداء المالي: الدور المعدل لجودة التدقيق الخارجي (رسالة ماجستير غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.
14. العمري، نور محمد، و كلبونة، أحمد يوسف. (2022). أثر إدارة المخاطر الائتمانية في تحسين أداء البنوك التجارية الأردنية: حسب بطاقة الأداء المتوازن (رسالة ماجستير غير منشورة). جامعة البلقاء التطبيقية، السلط.
15. العنبورية، سارة بنت علي بن ناصر، و الجهاني، عبدالناصر السيد محمد. (2023). المسؤولية الدولية الجنائية عن الهجمات السيبرانية أثناء النزاعات المسلحة (رسالة ماجستير غير منشورة). جامعة السلطان قابوس.

16. عوض، راما محمود جوهر، و خشمان، أيسر محمد علي. (2022). أثر الذكاء الاستراتيجي في إدارة المخاطر في المستشفيات الخاصة الأردنية (رسالة ماجستير غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.

17. القحطاني، محمد عبدالهادي ظافر العرجي، و أبو قاعد، غازي رسمي عايد. (2023). أثر القدرات الديناميكية في إدارة المخاطر السيبرانية: المرونة الاستراتيجية متغيرا وسيطا: دراسة تطبيقية في وزارة الداخلية في دولة قطر (رسالة دكتوراه غير منشورة). جامعة مؤتة، مؤتة.

18. القحطاني، محمد عبدالهادي ظافر العرجي، و أبو قاعد، غازي رسمي عايد. (2023). أثر القدرات الديناميكية في إدارة المخاطر السيبرانية: المرونة الاستراتيجية متغيرا وسيطا: دراسة تطبيقية في وزارة الداخلية في دولة قطر (رسالة دكتوراه غير منشورة). جامعة مؤتة، مؤتة.

19. المري، حمد سالم، القعيد، مرزوق عايد، و الصوالحة، أيوب أحمد محمد. (2020). أثر إدارة المخاطر على الأداء الاستراتيجي: ذكاء الأعمال كمتغير وسيط في البنوك التجارية العاملة في دولة الكويت (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.

20. المعايطه، أسيل يحيى، و المخادمة، أحمد عبدالرحمن كريم. (2023). أثر إدارة المخاطر التشغيلية في دعم الميزة التنافسية: دراسة تطبيقية على البنوك التجارية العاملة في الأردن (رسالة ماجستير غير منشورة). جامعة مؤتة، مؤتة.

21. المقدشي، على حسين علي، و القرشي، عبدالله علي. (2019). أثر إدارة المخاطر المصرفية على ربحية البنوك اليمنية: دراسة مقارنة بين البنوك التجارية والإسلامية (رسالة ماجستير غير منشورة). جامعة الأندلس للعلوم والتقنية، صنعاء.

22. النجار، عمر محمد خليل، و الفرا، ماجد محمد عبدالسلام. (2019). أثر إدارة المخاطر على التميز المؤسسي لجامعة الأقصى بقطاع غزة (رسالة ماجستير غير منشورة). الجامعة الإسلامية (غزة)، غزة.

ثانيا: المراجع باللغة الإنجليزية

1. Abdul Jader, Ahmed Maysar. (2022). Factors Affecting the Behavioral Intention to Adopt Web-Based Recruitment in Human Resources Departments in Telecommunication

- Companies in Iraq. Anbar University Journal of Economic and Administrative Sciences, Vol. 14, No. 2, 404-416.
2. Abu Alead, R. M. S., and Ab Altalibe, A. A. (2023). Attribution Challenges in the Era of Cyber Warfare: Unraveling the Identity of Cyber-Attackers. Journal of the Higher Institute for Qualitative Studies, Vol. 3, No. 16, 5287-5309.
 3. Abu Aliqa, Roaa Yousef, and Attir, Mohammed Abdullah Aref. (2023). An Enhanced Gazelle Optimization Algorithm for Intrusion Detection System in Wireless Sensor Networks (Unpublished Master's Thesis). Arab Open University, Amman.
 4. Ahmed, Maqbool, Kazar, Aqaba, and Harous, Saad. (2024). Generative Artificial Intelligence for Cyber Security: Literature Review and Challenges. Scientific Journal of Saba Region University, Vol. 7, No. 2, 425-470.
 5. Al-Amri, Samah Khaled Ibrahim, and Sweidan, Andraos Issa. (2019). Analysis and Synthesis of Efficient Intrusion Detection System in Internet of Things (Unpublished Master's Thesis). University of Jordan, Amman.
 6. Al-Balawi, Khalaf bin Mohammed. (2025). Opportunities for Cyber Insurance to Address the Challenges of Cyber Attacks: Repercussions for SMEs. University of Sharjah Journal of Legal Sciences, Vol. 22, No. 1, 560-607.
 7. Albalushi, J. K. J., Ali, S., and Aman, W. (2022). Proposed Enhanced Systematic Approach of Impact Analysis Process for Cyber-Attacks on Distributed Control Systems (Unpublished Master's Thesis). Sultan Qaboos University, Muscat.
 8. Al-Dhawadi, Mahmoud Abdel Salam. (2020). The Third Human Dimension' Paradigm: A New Intellectual Framework for the Promotion of Cultural Sociology. Journal of Arts, Vol. 32, No. 1, 1-11.

9. Al-Masry, Baha Nayef Ismail, and Jaradat, Ghaith Mohammed. (2022). Sperm Swarm Optimization Algorithm for Intrusion Detection System in Wireless Sensor Networks (Unpublished Master's Thesis). Arab Open University, Amman.
10. Al-Muadat, Amna Awad, Bani Ahmed, Suleiman Ahmed, and Al-Durgham, Osama Mohammed Ahmed. (2023). Prediction of Cyber Attacks on the Cloud Computing Services for Big Data Applications (Unpublished Master's Thesis). Al-Balqa Applied University, As-Salt.
11. Al-Muadat, Amna Awad, Bani Ahmed, Suleiman Ahmed, and Al-Durgham, Osama Mohammed Ahmed. (2023). Prediction of Cyber Attacks on the Cloud Computing Services for Big Data Applications (Unpublished Master's Thesis). Al-Balqa Applied University, As-Salt.
12. Al-Quraan, Rabi' Sufyan Tayseer, and Obaidat, Ibrahim Muhammad Salem. (2023). Modeling and Simulation of New AI Technique to Address and Limit Cyber Attacks: ChatGPT Experimental Based (Unpublished Master's Thesis). Hashemite University, Zarqa.
13. Al-Ramadan, Bashayer Adnan, Shahid, Mohammed, Kapila, Kosem, and Al-Fadhli, Suad Mohammed. (2022). The Correlation of High-Risk Human Papillomavirus "HR-HPV" with Lesion Progression and other Risk Factors (Unpublished Master's Thesis). Arabian Gulf University, Manama.
14. Al-Salahi, Fatima Abdullah, and Al-Tarawneh, Alaa Al-Din Awad. (2024). Factors Affect Economic Well-Being: Human Developing Index for Selected Arab Countries. Jordanian Journal of Economic Sciences, Vol. 11, No. 1, pp. 24-34.

15. Al-Tamimi, Omar Ahmed, and Mughaid, Alaa Saeed Mohammed. (2024). A Novel Cyber Techniques for Detecting and Preventing Phishing Attacks Using AI (Unpublished Master's Thesis). Hashemite University, Zarqa.
16. Al-Tarawneh, Ghosoun Khalaf Firas, Al-Jubouri, Salloum Ahmed Dawood, and Al-Maaytah, Omar Nawaf Khaled. (2020). Impact of Human Factors on Quality Improvement of Production Systems (Unpublished Master's Thesis). Mutah University, Mutah.
17. Al-Zakwani, Alia Saeed, Zidoun, H. M., and Al-Hamadani, A. (2024). Phishing Attack Detection: A Comparative Study of Fully Connected Networks, Long Short Term Memory and Convolutional Neural Networks on the Eurepoc Dataset (Unpublished Master's Thesis). Sultan Qaboos University, Muscat.
18. Attia, Zaid Ramzi Hashem, Obaidat, Maher Suleiman, and Al-Saghir, Maher Abdul-Moneim. (2024). Expression of Human Epidermal Growth Factor Receptor 2 "HER2" in Colorectal Cancer and its Correlation with Clinicopathological Characteristics among Jordanian Patients (Unpublished Master's Thesis). Al-Balqa' Applied University, As-Salt.
19. Awad, Lana Nabil Hussein, and Al-Khazaali, Ziad Ali Fadl. (2022). Critical Factors that Affect the Adoption of Human Resource Information Systems "HRIS" in the International Organizations for Migration (Unpublished Master's Thesis). Al-Ahliyya Amman University, Salt.
20. Badran, A., Abdel Gaber, S., and Haggag, R. (2024). Proposed Cyber Security Framework for Reducing the Security Risks on the Egyptian Petroleum Sector. Scientific Journal of Business Research and Studies, Vol. 38, No. 3, 1247-1301.

21. Bouziane, S., and Latreche, T. (2025). Cyber Assurance and Cyber Risk Management: A Critical Analysis of the Leading Low-Cost Product in Algeria. *Journal of Contemporary Business and Economic Studies*, Vol. 8, No. 1, 310-332.
22. Debbache, H. S. L. N., Roula, D., and Benfenatki, N. (2023). Factors Influencing the Clinical Internship: A Survey of 3rd Year Medical Students at the Faculty of Medicine of Constantine. *Horizons for Science Journal*, Vol. 8, No. 4, 216-225.
23. Dohi, Surour Abdul-Hussein. (2024). The Web Graph on Page, Host and Cyber Attacks. *Journal of Sustainable Studies*, Vol. 6, Supplement, 1071-1099.
24. Hamed, S. M. S. H. (2023). Social Factors and Dialect Variation: An Analysis of Age, Gender, and Social Class in Linguistic Practice. *North European Academic Peer Review Journal for Studies and Research*, Vol. 4, No. 21, 243-269.
25. Ismail, H. S. G. (2020). Students' Cyber-Bullying of Secondary Schools Teachers as a Form of Social Exclusion in Saudi Arabia since the Outbreak of COVID-19. *Journal of the College of Education*, Vol. 78, No. 2, 65-111.
26. Laib, S. (2021). The Importance of Cyber Security in the Financial Sector in the Age of Digital Transformation. *Al-Asil Journal of Economic and Administrative Research*, Vol. 5, No. 1, 448-464.
27. Maqbul, M. Y. (2024). Factors Affecting Employees Motivation: An Exploratory Study of Employees at the General Administration of Education in Jeddah. *Arab Journal of Scientific Publishing*, No. 73, 71-96.
28. Metwally, A. B. M., Abdelazim, S. I., and Almarji, M. T. (2022). Internal Auditors' Role In Confronting Cyber and Fraud Risks Related to Outsourcing Insurance: An Exploratory Study. *Alexandria Journal of Accounting Research*, Vol. 6, No. 3, 1-31.

29. Ramadan, F. A. (2022). Outbreak Narratives and Medical Humanities: A Transdisciplinary Comparative Approach to the Literary Representation of Ebola in Preston's the Hot Zone (1994) and Tag Elsir's Ebola 76 (2012). College of Arts Journal, Volume 14, No. 2, 658-706.
30. Salim, A. T., and Khammas, B. M. (2023). Simplified Review on Cyber Security Threats Detection in IoT Environment Using Deep Learning Approach. Journal of the College of Basic Education, No. 119, 22-49.

الملاحق

استمارة استبيان

السلام عليكم ورحمة الله وبركاته

أخي الكريم / أختي الكريمة

تحية طيبة وبعد،

يقوم الباحثين بإجراء دراسة حول قياس أثر إدارة مخاطر العامل البشري على الحد من الهجمات السيبرانية: دراسة ميدانية على المؤسسات الحكومية في المملكة العربية السعودية

ونظراً لما لديكم من المعرفة العلمية والخبرة العملية ذات الصلة بموضوع البحث، نأمل الحصول منكم على العون والمساعدة في توفير المعلومات المناسبة لأغراض البحث، من خلال التكرم بإبداء رأيكم بالتأشير على الإجابة المناسبة من وجهة نظركم.

وأتقدم لحضراتكم بجزيل الشكر والتقدير للمساهمة في جهودكم في تعبئة هذا الاستبيان علماً أن جميع البيانات التي سيتم الحصول عليها منكم ستعامل بسرية تامة، ولن تستخدم لغير أغراض هذا البحث، وسوف أزدكم بنتائج هذه الدراسة حال اكتمالها إن شاء الله.

وتفضلوا بقبول فائق التقدير والاحترام

أولاً: البيانات الشخصية

1- النوع الاجتماعي ☐ ذكر ☐ أنثى

2- العمر ☐ 25 سنة فأقل ☐ من 25 – 35 سنة ☐ من 35 – 45 سنة ☐ من 45 سنة فأكثر

3- المؤهل العلمي ☐ ثانوي ☐ بكالوريوس ☐ ماجستير ☐ دكتورة

4- الوضع المهني ☐ مدير ☐ نائب مدير ☐ رئيس قسم

ثانيا محاور الاستبيان

🌸 المحور الأول: إدارة مخاطر العامل البشري ، ضع إشارة (√) في المربع المناسب لاختيارك:

معارض بشدة	معارض	محايد	أو افق	أو افق بشدة	البعد
تحديد وتقييم المخاطر					
					تقوم المؤسسة بتحديد المخاطر البشرية المحتملة التي قد تؤثر على أمن المعلومات.
					يتم تقييم تأثير العامل البشري ضمن تحليل شامل لمصادر التهديد السيبراني.
					تُستخدم أدوات تقييم مهنية لرصد السلوكيات البشرية التي قد تؤدي إلى اختراقات أمنية.
					تعتمد المؤسسة على بيانات سابقة لتحليل الحوادث المرتبطة بالعامل البشري.
					يتم تضمين الموظفين في عمليات تحديد المخاطر المتعلقة بالأمن السيبراني.
معالجة إدارة المخاطر					
					توفر المؤسسة برامج تدريبية متخصصة للتقليل من أخطاء العامل البشري.
					توجد سياسات واضحة للتعامل مع السلوكيات التي تهدد أمن المعلومات.
					يتم تطوير خطط عمل لمعالجة الثغرات التي يسببها العامل البشري.

معارض بشدة	معارض	محايد	أو افق	أو افق بشدة	البعد
					تعتمد المؤسسة حلولاً تقنية تقلل من احتمالية حدوث الخطأ البشري.
					تُشرك إدارة الموارد البشرية في خطط تقليل المخاطر السيبرانية الناتجة عن الموظفين.
مراقبة إدارة المخاطر					
					تراقب المؤسسة بشكل دوري سلوك الموظفين المتعلق باستخدام الأنظمة الإلكترونية.
					توجد آليات إنذار مبكر لاكتشاف أي نشاط غير معتاد ناتج عن العنصر البشري.
					يتم تحديث إجراءات المراقبة بشكل دوري لمواكبة تطور التهديدات البشرية.
					يتم توثيق ومراجعة حوادث الاختراق الناتجة عن العامل البشري بشكل منتظم.
					يتم إعداد تقارير دورية حول التزام الموظفين بسياسات الأمن السيبراني.

✿ المحور الثاني: الحد من الهجمات السيبرانية، ضع إشارة (✓) في المربع المناسب

لاختيارك:

المعيار	أوافق بشدة	أوافق	محايد	معارض بشدة	معارض بشدة
تمتلك المؤسسة خطة استجابة واضحة للهجمات السيبرانية.					
تُحدَّث أنظمة الحماية بشكل مستمر لتقليل احتمالية الهجمات.					
تعتمد المؤسسة على أدوات متقدمة لرصد التهديدات السيبرانية.					
يتم اختبار أنظمة الأمن السيبراني بانتظام للتأكد من كفاءتها.					
يتم التعامل مع أي محاولة اختراق بسرعة وفعالية.					
توجد آليات تحقق متعددة الهوية (MFA) لحماية الأنظمة.					
تُجرى محاكاة دورية لهجمات سيبرانية للتدريب على مواجهتها.					
تُستخدم حلول تشفير قوية لحماية البيانات الحساسة.					
يتم تقييم المخاطر السيبرانية الجديدة عند كل تحديث للنظام.					

معارض بشدة	معارض	محايد	أو افق	أو افق بشدة	البعد
					تعتمد المؤسسة إجراءات صارمة للحد من وصول غير المصرح به إلى المعلومات.
					تمتلك المؤسسة خطة استجابة واضحة للهجمات السيبرانية.
					تُحدَّث أنظمة الحماية بشكل مستمر لتقليل احتمالية الهجمات.
					تعتمد المؤسسة على أدوات متقدمة لرصد التهديدات السيبرانية.
					يتم اختبار أنظمة الأمن السيبراني بانتظام للتأكد من كفاءتها.

مع خالص التقدير والاحترام

Mid-Ocean University

College of Management



Master's Degree in Risk Management for Graduates

**" The Impact of Human Factor Risk Management on
Reducing Cyber Attacks: A Field Study of Government
Institutions in the Kingdom of Saudi Arabia"**

Preparation:

Walid Nabil Alkabbani

2021201871

Supervision:

Dr. Al-Faisal Abdelhamid Mohamed Hassan

1447 – 2025