International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (3), No. (10)
IJFAES
October 2024
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (3)، العدد (10)

الاستراتيجيات الفعالة لإدارة المخاطر والتخفيف منها في مجال أمن الشركات في المملكة العربية السعودية

خالد عبده خبراني
ماجستير إدارة الأعمال، كلية الإدارة، جامعة ميد أوشن، الإمارات العربية المتحدة
Khubrani388@gmail.com

أسماء أبو عنزه
كلية الإدارة، جامعة ميد أوشن، الإمارات العربية المتحدة

المستخلص

تتناول هذه الدراسة إدارة المخاطر وتعزيز الأمن السيبراني في الشركات السعودية، حيث تعد هذه القضية من التحديات الحيوية التي تواجه المؤسسات في ظل التحول الرقمي المتسارع. تهدف الدراسة إلى تحليل استراتيجيات إدارة المخاطر المتبعة في الشركات السعودية وكيفية تعزيزها للأمن السيبراني لحماية البيانات والأصول الحيوية. تم استخدام منهجية بحث متعددة الجوانب، تشمل المنهج الوصفي لتحليل الوضع الحالي لإدارة المخاطر، والمنهج الكمي لجمع البيانات من خلال استبيانات ومسوحات، والمنهج النوعي من خلال مقابلات مع خبراء في مجال الأمن السيبراني. تم التركيز على دراسة أهم المخاطر التي تواجه الشركات السعودية، سواء كانت تقنية، مالية، أو تنظيمية، وتحديد الأدوات والتقنيات المستخدمة للتخفيف من تأثير هذه المخاطر. تشمل النتائج تسليط الضوء على فعالية التدابير الوقائية المتبعة، مثل استخدام أنظمة المراقبة الأمنية، والتشفير، والتدريب المستمر للموظفين. كما تطرقت الدراسة إلى التحديات التي تواجه الشركات في تطبيق استراتيجيات الأمن السيبراني، خاصة في ظل التغير المستمر في طبيعة التهديدات السيبرانية. خلصت الدراسة إلى أن الشركات السعودية بحاجة إلى تبني استراتيجيات متكاملة لإدارة المخاطر، تتضمن تعزيز الوعي بين الموظفين، التعاون مع الجهات الحكومية والخاصة، وتوظيف تقنيات الذكاء الاصطناعي لمواجهة التهديدات المستقبلية. كما أوصت الدراسة بضرورة تحسين سياسات الأمن السيبراني وتحديثها بشكل مستمر لضمان حماية الأصول الرقمية والحفاظ على استمرارية الأعمال في مواجهة الأزمات السيبرانية.

الكلمات المفتاحية: إدارة المخاطر، الأمن السيبراني، التحول الرقمي، أنظمة المراقبة الأمنية.

International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (3), No. (10)
IJFAES
October 2024
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (3)، العدد (10)

Effective Strategies for Risk Management and Mitigation in the Field of Corporate Security in the Kingdom of Saudi Arabia

Khaled Abdo Khabarani
Master of Business Administration, College of Management, Midocean University, United Arab Emirates
Khubrani388@gmail.com

Asmaa Abuanza
College of Management, Mid Ocean University, United Arab Emirates

Abstract

This study addresses risk management and the enhancement of cybersecurity in Saudi companies, a critical issue in the face of rapid digital transformation. The research aims to analyze the risk management strategies employed by Saudi companies and how these strategies enhance cybersecurity to protect vital data and assets. A multi-faceted research methodology was utilized, incorporating descriptive analysis to evaluate the current risk management situation, quantitative methods through surveys and questionnaires, and qualitative interviews with cybersecurity experts .The study focused on identifying the major risks faced by Saudi companies, whether technological, financial, or organizational, and the tools and technologies used to mitigate these risks. The results highlighted the effectiveness of preventive measures such as the use of security monitoring systems, encryption, and continuous employee training. The study also explored the challenges companies face in implementing cybersecurity strategies, particularly given the evolving nature of cyber threats. The study concluded that Saudi companies need to adopt integrated risk management strategies, which include raising employee awareness, collaborating with governmental and private entities, and utilizing artificial intelligence technologies to address future threats. The study also recommended

continuous improvement and updating of cybersecurity policies to ensure the protection of digital assets and maintain business continuity in the face of cyber crises.

Keywords: Risk Management, Cybersecurity, Digital Transformation, Security Monitoring, Systems.

الفصل الأول

المقدمة

تعتبر إدارة المخاطر في الشركات مجالاً حيوياً، لا سيما في المملكة العربية السعودية حيث يشهد السوق تنوعًا وتطورًا مستمرين. يواجه القطاع الخاص مجموعة من التحديات التي تشمل المخاطر المالية، التشغيلية، الأمنية، والسيبرانية. تتطلب هذه التحديات تطبيق استراتيجيات فعالة لإدارة المخاطر تضمن استمرارية الأعمال وحمايتها من التهديدات المحتملة. تتضمن إدارة المخاطر عملية منهجية لتحديد وتحليل وتقييم المخاطر، ثم وضع خطط للتخفيف من آثارها والتحكم فيها، إن الخطوة الأولى في إدارة المخاطر هي التقييم الشامل. يشمل هذا التقييم تحديد جميع المخاطر المحتملة التي قد تواجهها الشركة وتحليل تأثيرها المحتمل، وبعد تحديد المخاطر، يتم وضع خطط وقائية لمواجهتها قبل أن تتحول إلى أزمات. تشمل هذه الخطط وضع سياسات وإجراءات للتعامل مع الحوادث الأمنية والطوارئ. كما يتم تطوير خطط استجابة سريعة للتعامل مع الأزمات عند وقوعها، مما يضمن استمرارية العمل وتقليل الخسائر. (الجهني، 2017)

تعتبر التوعية والتدريب جزءاً أساسياً من استراتيجية إدارة المخاطر حيث ذكرها (العمري، 2021) وذكر أنه يجب تدريب الموظفين على السياسات والإجراءات الأمنية، وكذلك زيادة وعيهم بالمخاطر المحتملة وكيفية التعامل معها. يمكن تنظيم ورش عمل ودورات تدريبية دورية لتعزيز ثقافة الأمان في الشركة، كما أن التكنولوجيا تلعب دوراً محورياً في إدارة المخاطر. يمكن استخدام الأنظمة الأمنية المتقدمة مثل أنظمة الكشف عن الاختراق وأنظمة إدارة الهوية والوصول لحماية البيانات والمعلومات الحساسة.

كما يمكن استخدام برامج الذكاء الاصطناعي لتحليل البيانات والكشف المبكر عن التهديدات. والتعاون مع الجهات الخارجية مثل الجهات الحكومية وشركات الأمن الخاصة يمكن أن يكون فعالًا في إدارة المخاطر. يمكن لهذه الجهات تقديم الخبرات والدعم اللازمين لتحسين إجراءات الأمن والحماية، إن أحد

الاستراتيجيات الفعالة للتخفيف من المخاطر المالية هو تنويع الاستثمارات والموارد. يساعد هذا التنويع في تقليل تأثير الخسائر المالية المحتملة.

وهذا يحدث عن طريق توزيع المخاطر عبر مجالات مختلفة، ولذلك تعتبر التأمينات أحد الأدوات الفعالة للتخفيف من المخاطر. يمكن للشركات الحصول على تأمينات تغطي مجموعة متنوعة من المخاطر مثل التأمين ضد الكوارث الطبيعية، والتأمين الصحي للموظفين، والتأمين ضد الاختراقات السيبرانية. (خالد، 2021)

ويمكن للشركات تحقيق مستوى عالٍ من الأمن والاستقرار من خلال تبني استراتيجيات فعالة لإدارة المخاطر. من خلال التقييم الشامل، والتخطيط الوقائي، واستخدام التكنولوجيا المتقدمة، والتدريب المستمر، يمكن للشركات تحسين قدرتها على مواجهة التحديات وضمان استمرارية أعمالها. تواجه الشركات في المملكة العربية السعودية بيئة أعمال مليئة بالتحديات والفرص على حد سواء. مع التطور السريع في التكنولوجيا وزيادة التهديدات الأمنية، أصبحت إدارة المخاطر جزءًا لا يتجزأ من استراتيجيات الشركات لضمان استمرارية العمل وحمايته من التهديدات المختلفة. يتضمن ذلك التعامل مع المخاطر المالية، التشغيلية، الأمنية، والسيبرانية بشكل منهجي وفعال. (الراشد، 2017)

حيث يوجد عدة أخطار لهذه تواجه هذه الشركات (الحسن، 2015)، ومنها الأخطار المالية التي تتمثل في عدم الاستقرار الاقتصادي، التغيرات في أسعار الصرف والفوائد، وتقلبات السوق المالية. قد تؤدي هذه المخاطر إلى خسائر مالية كبيرة تؤثر على قدرة الشركة على تحقيق أرباحها واستمراريتها. ومنها المخاطر التشغيلية التي تتعلق بالأخطاء البشرية، الأعطال التكنولوجية، والنقص في الموارد. يمكن لهذه المخاطر أن تؤدي إلى توقف العمليات وتأخير الإنتاج، مما يؤثر على سمعة الشركة وعلاقتها بعملائها.

مشكلة الدراسة

تتمثل المشكلة الرئيسية لهذه الدراسة في عدم كفاية الاستراتيجيات الحالية لإدارة المخاطر في العديد من الشركات السعودية. بالرغم من الجهود المبذولة، لا تزال هناك فجوات كبيرة في كيفية التعامل مع المخاطر المختلفة، مما يعرض هذه الشركات لمجموعة متنوعة من التهديدات. تتعدد أسباب هذه الفجوات وتشمل نقص الوعي بالمخاطر، التغيرات السريعة في البيئة التكنولوجية، وكذلك التغيرات المستمرة في القوانين واللوائح التنظيمية.

من هذه المخاطر التي تهدد أمن الشركات السعودية المخاطر المالية التي تتمثل في التغيرات في أسعار الصرف، تقلبات السوق، والتغيرات في أسعار الفائدة. هذه المخاطر يمكن أن تؤدي إلى تقلبات كبيرة في الإيرادات والأرباح، (العمرو، 2020)، مما يؤثر بشكل مباشر على الاستقرار المالي للشركة، ويمكن أن تؤدي التغيرات المفاجئة في أسعار النفط إلى تقلبات حادة في الإيرادات للشركات العاملة في قطاع الطاقة. بالإضافة إلى ذلك، يمكن للتغيرات في أسعار الفائدة أن تؤثر على تكلفة التمويل والقروض، مما يزيد من أعباء الديون على الشركات.

من المخاطر التي تهدد الشركات هي المخاطر الأمنية أي هي التهديدات الفيزيائية مثل السرقة والتخريب، وكذلك التهديدات السيبرانية مثل الاختراقات والهجمات الإلكترونية. تتطلب هذه المخاطر استراتيجيات حماية فعالة لضمان سلامة الأصول المادية والبيانات الحساسة، وتعتبر الهجمات السيبرانية من أبرز التهديدات الأمنية التي تواجه الشركات في المملكة. يمكن لهذه الهجمات أن تؤدي إلى سرقة البيانات الحساسة أو تعطيل الأنظمة الحيوية، مما يسبب خسائر مالية كبيرة ويضر بسمعة الشركة.

وتأتي المخاطر السيبرانية الهجمات الإلكترونية، البرمجيات الخبيثة، وسرقة البيانات. في العصر الرقمي، أصبحت هذه المخاطر من أخطر التهديدات التي تواجه الشركات، حيث يمكن أن تؤدي إلى خسائر مالية كبيرة وتضر بسمعة الشركة، وتتضمن الهجمات عبر البرمجيات الخبيثة (مثل الفيروسات وأحصنة طروادة)، وهجمات الفدية التي تطالب بفدية لإعادة الوصول إلى البيانات أو الأنظمة المحتجزة، والهجمات التي تستهدف سرقة البيانات الحساسة من الشركات. (سالم، 2017)

تشهد المملكة العربية السعودية تغيرات مستمرة في القوانين واللوائح التنظيمية. يتطلب الامتثال لهذه التغيرات تعديل سياسات وإجراءات الشركات بشكل مستمر، مما يمثل تحديًا كبيرًا لإدارة المخاطر، وتتضمن على التغيرات التنظيمية التعديلات في القوانين المتعلقة بحماية البيانات، وزيادة متطلبات الامتثال للمعايير الدولية، وكذلك التغيرات في السياسات الاقتصادية التي تؤثر على العمليات التجارية. (محمد، 2016)

تشير الأدلة إلى أن العديد من الشركات في المملكة لا تزال تعتمد على استراتيجيات إدارة مخاطر تقليدية وغير كافية. تشمل هذه الاستراتيجيات الاعتماد الكبير على التأمين، وضعف استخدام التكنولوجيا المتقدمة، وقلة التدريب والتوعية، حيث تشمل الثغرات الرئيسية في الاستراتيجيات الحالية نقص التكامل بين أنظمة إدارة المخاطر، الاعتماد المفرط على الإجراءات الورقية، وعدم كفاية الاستجابة السريعة للأزمات. هذا يعرض الشركات لخطر الفشل في مواجهة التهديدات الجديدة والمعقدة، تتضمن الاستراتيجيات المتكاملة لإدارة

المخاطر تحليل المخاطر بشكل شامل، وتطوير خطط وقائية واستجابة فعالة، واستخدام التكنولوجيا المتقدمة، وزيادة الوعي والتدريب. هذه الاستراتيجيات تساعد في تحسين كفاءة العمليات وتقليل تأثير المخاطر، ويمكن تطبيق الاستراتيجيات المتكاملة من خلال اعتماد نهج شامل يشمل جميع جوانب إدارة المخاطر. يجب أن تتضمن هذه الاستراتيجيات تحديد المخاطر، تقييمها، وضع خطط وقائية واستجابة، وتنفيذ برامج تدريب وتوعية مستمرة. (عبدالعزيز، 2016)

أهمية الدراسة

- **الأهمية العلمية:**

تنبع الأهمية العلمية لهذه الدراسة من الحاجة الملحة لفهم أعمق لتأثير إدارة المخاطر على نجاح المشاريع في الشركات في المملكة العربية السعودية. تسهم هذه الدراسة في سد الفجوة البحثية القائمة في الأدبيات الحالية، من خلال تقديم: (البقمي، 2019)

رؤية شاملة حول كيفية تأثير تحديد المخاطر وتقييم المخاطر والاستجابة للمخاطر ومراقبة المخاطر والسيطرة عليها على نجاح المشاريع. علاوة على ذلك؛ تهدف الدراسة إلى تحليل الفروق الديموغرافية مثل الجنس؛ والعمر والمؤهل العلمي؛ والمسمى الوظيفي، وسنوات الخبرة؛ مما يتيح فهماً أكثر دقة وشمولية للعوامل التي تؤثر على تقييم المبحوثين لإدارة المخاطر ونجاح المشاريع.

تضيف هذه الدراسة إلى المعرفة الأكاديمية في مجالي إدارة المخاطر وإدارة المشاريع؛ من خلال تقديم نتائج تحليلية تستند إلى بيانات ميدانية. يسهم هذا في تطوير نظريات ومفاهيم جديدة؛ يمكن أن تستخدم كأساس للأبحاث المستقبلية. كما أن استخدام المنهج الوصفي الكمي والتحليل الإحصائي يمكن أن يعزز من مصداقية وموثوقية النتائج» مما يسهم في إثراء الأدبيات الأكاديمية ببيانات دقيقة ومعمقة. (سالم، 2017)

- **الأهمية العملية:**

من الناحية العملية؛ توفر هذه الدراسة رؤى وتوصيات يمكن أن تكون ذات فائدة كبيرة للمديرين وأصحاب القرار في الشركات السعودية بالمنطقة. وتحديد المخاطر وتقييمها والاستجابة لها ومراقبتها ليمت مجرد نظريات أكاديمية؛ بل هي أدوات أساسية يمكن استخدامها لتحسين أداء المشاريع وزيادة

فرص نجاحها. على سبيل المثال يمكن أن تساعد نتائج الدراسة في تحسين عمليات التخطيط والتنفيذ من خلال توفير إطار عمل واضح ومحدد لإدارة المخاطر. (فهد، 2019)

تساعد هذه الدراسة الشركات في تحديد النقاط الحرجة في إدارة المخاطر وتطوير استراتيجيات فعالة للتعامل معها. يمكن أن يؤدي ذلك إلى تقليل المخاطر المحتملة؛ وتعزيز الشفافية والاستخدام الأمثل للموارد مما ينعكس إيجابياً على خفض التكاليف وتحقيق الأهداف المحددة للمشاريع. كما أن تحليل الفروق الديموغرافية يوفر فهماً أعمق لتأثير العوامل الشخصية على تقييم المبحوثين لإدارة المخاطر مما يمكن أن يساعد في تطوير برامج تدريبية وتوعوية تستهدف تحسين قدرات ومهارات الموظفين في هذا المجال.

أهداف الدراسة

من أهم أهداف تلك الدراسة أنها تقوم بما يلي:

- **تحليل التهديدات والضعف**: الهدف الرئيسي هو تحليل التهديدات الحالية والمحتملة التي تواجه الشركات في المملكة العربية السعودية، بما في ذلك التهديدات السيبرانية والفيزيائية، وتحديد الضعف في نظم الأمان الحالية.
- **تطوير استراتيجيات الأمن**: وضع استراتيجيات فعالة تهدف إلى حماية البيانات والمعلومات الحساسة، وتعزيز الأمن الرقمي والفيزيائي للشركات، بما يشمل وضع سياسات صارمة وإجراءات محكمة.
- **تعزيز الوعي والتدريب**: تعزيز وعي الموظفين بأهمية الأمن والسلامة، وتوفير التدريب المستمر لهم للتعرف على أحدث التقنيات والممارسات في مجال الأمن. (عبد العزيز، 2016)
- **استخدام التكنولوجيا المتقدمة:** تطبيق أحدث التقنيات المتقدمة في مجال الأمن مثل أنظمة الكشف عن التسلل والحماية من البرمجيات الخبيثة، لتعزيز القدرة على اكتشاف واحتواء الهجمات بشكل فعال.
- **الامتثال للتشريعات الأمنية**: ضمان الامتثال للتشريعات الأمنية المحلية والدولية، وتطبيق المعايير القانونية والتقنية اللازمة لضمان الحماية القانونية والمالية للشركات.
- **تعزيز الاستجابة للأزمات**: تطوير استراتيجيات فعالة للتعامل مع الأزمات الأمنية والاستجابة السريعة لها، للحد من التأثيرات السلبية وضمان استمرارية الأعمال. (حامد، 2017)

- **تحسين الأداء العملياتي:** تحسين كفاءة وفعالية العمليات الأمنية داخل الشركات، وتعزيز التكامل بين أقسام الأمن والإدارات الأخرى لتعزيز التعاون والتنسيق.
- **تعزيز الثقة العامة:** بناء ثقة العملاء والشركاء والمستثمرين بفعالية الأمان والحماية التي توفرها الشركات، مما يسهم في تعزيز سمعتها وزيادة فرص النمو والاستثمار.
- **تعزيز الابتكار والتطوير:** تشجيع الشركات على الابتكار في حلول الأمن والتكنولوجيا، وتطوير الحلول المبتكرة التي تتكيف مع التهديدات المتغيرة والتطلعات المستقبلية. من خلال تشجيع البحث والتطوير، وتبني التقنيات والحلول الجديدة التي تظهر في السوق.
- **تحقيق الاستدامة الاقتصادية:** تعزيز الاستدامة الاقتصادية للشركات من خلال الحفاظ على الثروات والموارد وتقليل التكاليف الناجمة عن الاستجابة لحوادث الأمن، ولذلك فإنها تهدف إلى تحقيق أمان شامل واستقرار اقتصادي، وتعزيز قدرة الشركات على التكيف مع التحديات المتزايدة والمحافظة على استدامتها في السوق المحلي والعالمي. (حسن، 2018)
- **تحديد المخاطر الأمنية المحتملة:** إن هذه الدراسة تسعى إلى تحديد وفهم مجموعة المخاطر الأمنية المحتملة التي تواجه الشركات في المملكة. تشمل هذه المخاطر الهجمات السيبرانية، سرقة البيانات، الاختراقات، والتجسس الصناعي، ومنه إلى تحليل الوضع الحالي لإدارة أمن المعلومات في الشركات السعودية. يتضمن ذلك تقييم السياسات والإجراءات الحالية، البنية التحتية التقنية، والوعي الأمني بين الموظفين. (ناصر، 2018)
- **تطوير إطار عمل متكامل:** وهذا من خلال تطوير إطار عمل متكامل لإدارة المخاطر الأمنية يناسب البيئة السعودية. يشمل هذا الإطار السياسات والإجراءات، الحلول التقنية، وخطط الاستجابة للطوارئ.
- **تعزيز التعاون بين القطاعين العام والخاصة:** تتجه الدراسة نحو تعزيز التعاون بين القطاعين العام والخاص في مجال أمن المعلومات. يتضمن ذلك توصيات لتبادل المعلومات، تنظيم ورش عمل ومؤتمرات، وتطوير شراكات استراتيجية، وأيضا تعزيز قدرة الشركات على التكيف مع التهديدات الأمنية المتغيرة والمتطورة. يشمل ذلك تطوير استراتيجيات مرنة وقابلة للتعديل بشكل مستمر.

- **تحديد أفضل الممارسات العالمية**: من خلال استعراض أفضل الممارسات العالمية في مجال إدارة المخاطر الأمنية. يشمل ذلك تحليل استراتيجيات الشركات الرائدة دولياً والتوصيات الصادرة عن الهيئات والمنظمات المعنية بأمن المعلومات، كما يتم تقييم الاستثمارات الحالية في مجال الأمن وتقديم توصيات حول كيفية تحسينها. يشمل ذلك تحليل التكلفة والفائدة لبرامج وأدوات الحماية المختلفة. (الشمري، 2017)

تساؤلات الدراسة

من خلال مناقشة أهمية وأهداف هذه الدراسة، أقوم بطرح عدة أسئلة تفسر هذه النظرية ومنها:

أولاً: الأسئلة الرئيسية:

- ما هي التهديدات الرئيسية التي تواجه الشركات في مجال الأمن في السعودية؟ وكيف يؤثر التهديد السيبراني على أمن الشركات في المملكة العربية السعودية؟
- ما هي أبرز استراتيجيات إدارة المخاطر التي تستخدمها الشركات في المملكة العربية السعودية، وما هو دور التدريب والتوعية في تعزيز الأمن داخل الشركات؟

ثانياً: الأسئلة الفرعية:

- ما هي التقنيات المتقدمة التي يمكن استخدامها لتعزيز الأمن السيبراني في الشركات؟
- كيف يؤثر الامتثال للتشريعات الأمنية على استراتيجيات الشركات في السعودية؟
- ما هي أهمية بناء ثقة العملاء والشركاء في استراتيجيات إدارة المخاطر؟
- كيف يمكن للشركات تحقيق التوازن بين الأمن والابتكار في بيئة الأعمال؟ وما هي التحديات الرئيسية التي تواجه الشركات في تنفيذ استراتيجيات الأمن؟ وكيف يمكن للشركات تقييم فعالية استراتيجيات إدارة المخاطر التي تنفذها؟
- ما هو تأثير انتهاكات البيانات على الشركات وكيف يمكن التصدي لهذه الانتهاكات؟ وكيف يمكن للشركات تحديد مستوى التهديدات والمخاطر المحتملة لأمنها؟

فروض الدراسة

توضح هذه الفروض أهمية الدراسة في استكشاف وتحليل التحديات وتطوير الحلول لتحقيق أمن شامل واستقرار اقتصادي في السعودية، وتشتمل على: (الحربي، 2019)، (ماجد، 2018)

- **تحديد التهديدات الرئيسية**: من خلال الفرضيات، يتم التركيز على تحليل وتحديد التهديدات الأمنية الرئيسية التي تواجه الشركات في المملكة العربية السعودية، مثل الهجمات السيبرانية والتجسس الصناعي والتهديدات الفيزيائية. حيث تواجه الشركات في المملكة العربية السعودية مستوى متزايداً من التهديدات السيبرانية نتيجة للتحول الرقمي السريع والاعتماد المتزايد على التكنولوجيا، وتبحث الدراسة في مدى تأثير التحول الرقمي على زيادة التهديدات السيبرانية، بما في ذلك الهجمات الخبيثة وسرقة البيانات.
- **تقييم الضعف والفجوات**: دراسة مفصلة للضعف والفجوات في أنظمة الأمان الحالية للشركات، وذلك لتحديد المناطق التي تحتاج إلى تعزيز وتحسين لضمان الحماية الشاملة.
- **تطوير استراتيجيات مبتكرة**: تقديم فرضيات حول تطوير استراتيجيات مبتكرة لإدارة المخاطر والتخفيف منها، مثل تكامل التقنيات الحديثة وتعزيز التدابير الأمنية لتعزيز استجابة الشركات للتهديدات.
- **أهمية التدريب والتوعية:** يتعين أن يتضمن الفرض المؤهلات التي توضح أهمية التدريب المستمر للموظفين والتوعية بمخاطر الأمن، مما يساهم في تعزيز الثقافة الأمنية داخل الشركات.
- **المعايير الأمنية:** يتم تفصيل فروض حول أهمية الامتثال للمعايير الأمنية المحلية والدولية كجزء من استراتيجيات الأمن الشاملة للشركات.
- **التأثير على الاستدامة والنمو الاقتصادي**: يتضمن الفرض فحص التأثير الذي تخلفه استراتيجيات إدارة المخاطر على استدامة الأعمال والنمو الاقتصادي في المملكة العربية السعودية.
- **الحاجة للتقييم المستمر**: حيث التقييم المستمر لاستراتيجيات الأمن السيبراني يساعد في تحسينها وتكييفها مع التهديدات المتغيرة، وهذا يعرض من خلال أهمية التقييم المستمر وتقديم آليات فعالة لتنفيذه.

- **الابتكار والتطوير**: تسليط الضوء على دور الابتكار والتطوير في تطوير حلول جديدة وفعالة لإدارة المخاطر وتعزيز الأمن في الشركات.
- **تحقيق التوازن بين الأمن والأداء العملياتي**: تقديم دراسة حول كيفية تحقيق التوازن بين تعزيز الأمان وضمان استمرارية الأعمال وتحسين الأداء العملياتي للشركات.
- **تقييم أثر الاستراتيجيات**: يشمل الفرض تقييما لأثر الاستراتيجيات المقترحة على كفاءة وفعالية إدارة المخاطر وتحقيق الأهداف المحددة للأمن في الشركات.
- **نقص في الوعي الأمني بين موظفي الشركات السعودية**: مما يزيد من مخاطر الاختراقات الأمنية، وتقوم الدراسة بتقييم مستوى الوعي الأمني بين الموظفين ومدى تأثير هذا النقص على الأمان العام للشركات.
- **تأثير التكنولوجيا المتقدمة**: استخدام التكنولوجيا المتقدمة مثل الذكاء الاصطناعي والتحليل الكبير للبيانات يمكن أن يحسن بشكل كبير من إدارة المخاطر الأمنية، تناقش الدراسة كيفية تطبيق التكنولوجيا المتقدمة في تحسين أمن المعلومات وتخفيف المخاطر.
- **أهمية التدريب المستمر**: التدريب المستمر والتوعية الأمنية يمكن أن يقلل بشكل كبير من المخاطر الأمنية في الشركات السعودية، من خلالها يتم التأثير على برامج التدريب المستمر على الوعي الأمني وفعالية استراتيجيات إدارة المخاطر.
- **التعاون بين القطاعين العام والخاص**: وهذا يمكن أن يعزز من فعالية استراتيجيات إدارة المخاطر الأمنية، ويناقش هذا من خلال نماذج التعاون الناجحة وتقترح آليات لتعزيز هذا التعاون في المملكة.
- **أثر الجائحة على الأمن السيبراني**: جائحة كوفيد-19 أدت إلى تغييرات في بيئة العمل تسببت في زيادة التهديدات الأمنية للشركات. حيث تأثير الجائحة على الأمن السيبراني وكيفية تكيف الشركات مع هذه التحديات الجديدة.
- **التفاوت بين القطاعات**: هناك تفاوت في مستوى الأمن السيبراني بين مختلف القطاعات الاقتصادية في المملكة، يعالج ذلك بتحليل هذا التفاوت وتقديم توصيات لتحسين الأمن في القطاعات الأقل حماية.

- **نقص الموارد المالية:** نقص الموارد المالية المخصصة للأمن السيبراني في بعض الشركات يعوق تنفيذ استراتيجيات فعالة لإدارة المخاطر، وستبحث الدراسة في تأثير الميزانيات المحدودة على الأمن السيبراني وتقترح طرقًا لتخصيص الموارد بشكل أكثر فعالية.
- **أثر الثقافة التنظيمية**: توجد داخل الشركات وتؤثر على فعالية تنفيذ استراتيجيات الأمن السيبراني، حيث تحليل الثقافة التنظيمية وكيفية تحسينها لدعم استراتيجيات الأمن السيبراني.

الفصل الثاني: الإطار النظري

المصطلحات الخاصة بالدراسة

- **إدارة المخاطر (Risk Management):** عملية تحديد وتقييم ومعالجة المخاطر التي قد تؤثر على تحقيق أهداف المؤسسة. يشمل ذلك تحديد المخاطر المحتملة، تقييم تأثيرها، ووضع خطط للتعامل معها أو تخفيفها. وفقًا للجمعية الدولية لإدارة المخاطر (IRM)، تُعرف إدارة المخاطر بأنها: "التعرف المنهجي والتحليل والتحكم في المخاطر التي قد تؤثر على تحقيق أهداف المؤسسة." (IRM, 2018)

- **أمن الشركات (Corporate Security):** مجموعة من التدابير والإجراءات التي تتخذها الشركة لحماية أصولها المادية والرقمية، وكذلك بياناتها والعاملين بها من المخاطر المحتملة مثل السرقة، التهديدات السيبرانية، أو الهجمات الجسدية. (المجلس الدولي للأمن في الشركات، يُعرف أمن الشركات بأنه: "النظام الذي يحمي المؤسسات من الأخطار الداخلية والخارجية من خلال الجمع بين تكنولوجيا المعلومات وأمن الأفراد." (International Corporate Security Association, 2020)

- **استراتيجية (Strategy):** خطة طويلة الأمد يتم تطويرها لتحقيق أهداف محددة. في سياق إدارة المخاطر، الاستراتيجية تشير إلى تحديد وتطوير طرق للتقليل من المخاطر وتعظيم فرص النجاح. (لمايكل بورتر، "الاستراتيجية هي اختيار نهج معين لتحقيق التميز التنافسي وتحديد موقع الشركة مقارنة بمنافسيها." (Porter, 1996)

- **المخاطر السيبرانية (Cyber Risks):** تهديدات أو مخاطر تتعلق بأنظمة المعلومات والبنية التحتية الرقمية التي قد تؤثر على استمرارية عمل الشركة أو سرية البيانات. (بحسب المعهد الوطني للمعايير

والتكنولوجيا (NIST): "المخاطر السيبرانية هي مخاطر الأضرار التي قد تتعرض لها الأصول المعلوماتية بسبب الهجمات الإلكترونية." (NIST, 2012)

- **التخفيف من المخاطر (Risk Mitigation):** مجموعة من الإجراءات التي تتخذها المؤسسات لتقليل تأثير أو احتمالية حدوث المخاطر. (المنظمة المعايير الدولية (ISO): "التخفيف من المخاطر هو عملية تطوير وتنفيذ استراتيجيات وإجراءات لتقليل تأثير المخاطر." (ISO 31000, 2018)

- **الهجمات الإلكترونية (Cyber Attacks):** هي محاولات متعمدة لاختراق الأنظمة الرقمية أو الشبكات بغرض الوصول غير المصرح به إلى البيانات أو التسبب في تعطيل الأنظمة. (المركز الأمن السيبراني الأوروبي: "الهجوم الإلكتروني هو استخدام تكنولوجيا المعلومات للهجوم على الأنظمة أو الشبكات بهدف سرقة أو تعطيل أو تعديل البيانات." (ENISA, 2019)

- **التقييم الأمني (Security Assessment):** عملية تحليل وتقييم الوضع الأمني لمؤسسة أو نظام لتحديد النقاط الضعيفة وإجراءات التحسين. وفقًا لمركز أمن الإنترنت (CIS)، "التقييم الأمني هو أداة لتحديد الضعف المحتمل في الأنظمة وتحديد التهديدات المتوقعة." (CIS, 2019)

- **التخطيط للطوارئ (Contingency Planning):** وضع خطط استعداد لمواجهة الأحداث الطارئة أو الأزمات التي قد تؤثر على العمليات التشغيلية للمؤسسة (لوكالة الأمن القومي الأمريكية (NSA)): "التخطيط للطوارئ هو تطوير خطط بديلة لمعالجة الأزمات التي قد تؤثر على استمرارية العمليات." (NSA, 2017)

أنواع المخاطر في مجال أمن الشركات:

هذه الأنواع متعددة وتغطي نطاقًا واسعًا من التهديدات التي يمكن أن تواجه الشركات في العمليات اليومية، سواء على المستوى الداخلي أو الخارجي. هذه المخاطر تؤثر بشكل مباشر على استمرارية الأعمال، البيانات الحساسة، البنية التحتية، وسلامة الموظفين. إليك سرد مفصل لأنواع المخاطر التي تواجه الشركات في مجال الأمن، موثقة بمصادر مناسبة.

- **المخاطر التقنية (Technical Risks):** تشمل جميع التهديدات التي تتعلق بالبنية التحتية لتكنولوجيا المعلومات للشركة. تشمل هذه المخاطر الهجمات السيبرانية، الفيروسات، البرمجيات الخبيثة،

واختراقات البيانات. تعتبر الهجمات الإلكترونية، مثل هجمات الفدية (ransomware)، تهديدًا كبيرًا للشركات، حيث يمكن أن تؤدي إلى توقف الأنظمة بشكل كامل.

وهذا تبعا للتقرير السنوي للأمن السيبراني من منظمة ENISA، المخاطر التقنية تُعد من بين أكبر التهديدات التي تواجه الشركات اليوم نظرًا لاعتمادها الكبير على الأنظمة الرقمية. (ENISA, 2021)

- **المخاطر السيبرانية (Cybersecurity Risks):** هي فئة خاصة من المخاطر التقنية التي تتعلق بالتهديدات التي تستهدف أنظمة المعلومات، سواء عبر الإنترنت أو الشبكات الداخلية. تتضمن هذه المخاطر هجمات التصيد (phishing) وهجمات الاستيلاء على الحسابات والبيانات (account takeover). قد تؤدي هذه الهجمات إلى فقدان البيانات الشخصية أو التجارية الحساسة، مما يعرض الشركة لمخاطر مالية وقانونية. (تقرير مركز الأمن السيبراني الأوروبي (ENISA))، تزايدت المخاطر السيبرانية بشكل كبير خلال السنوات الأخيرة مع زيادة الهجمات الرقمية. (ENISA, 2019)

- **المخاطر المالية (Financial Risks):** هي تلك المخاطر المرتبطة بفقدان الأصول المالية للشركة نتيجة للاحتيال المالي، الهجمات السيبرانية التي تستهدف البيانات المالية، أو الأخطاء التشغيلية التي تؤدي إلى خسائر. كذلك يمكن أن تؤدي تقلبات السوق، مثل التغيرات في أسعار العملات أو التضخم المفاجئ، إلى تقليل القدرة المالية للشركات على الاستجابة للأزمات. (وفقًا لتقرير صادر عن معهد إدارة المخاطر، فإن الخسائر المالية المرتبطة بالاحتيال أو الهجمات الرقمية تعتبر تهديدًا رئيسيًا للشركات في القرن الحادي والعشرين. (IRM, 2019)

- **المخاطر التشغيلية (Operational Risks):** تشمل التهديدات التي تؤثر على سير العمل اليومي للشركات. قد تتضمن هذه المخاطر فشل النظام الداخلي، تعطل المعدات، أو حتى القرارات السيئة في الإدارة. هذا النوع من المخاطر يمكن أن يؤدي إلى توقف العمليات التجارية، وتأخير التسليمات، أو تقديم خدمات منخفضة الجودة. وهذا وفقًا لمعيار ISO 31000، المخاطر التشغيلية تمثل تهديدًا كبيرًا لاستمرارية الأعمال، وخاصة في الشركات التي تعتمد بشكل كبير على التكنولوجيا والبنية التحتية. (ISO 31000, 2018)

- **المخاطر القانونية (Legal Risks):** تشمل جميع التهديدات التي قد تنشأ عن عدم الامتثال للقوانين المحلية والدولية، أو من التورط في نزاعات قانونية. يمكن أن تتعرض الشركات لعقوبات وغرامات باهظة

في حالة انتهاكها للأنظمة المتعلقة بحماية البيانات، خصوصًا مع تطبيق قوانين مثل اللائحة العامة لحماية البيانات (GDPR) في أوروبا. (لدراسة من كلية الحقوق بجامعة هارفارد، تؤدي المخاطر القانونية إلى تأثير كبير على سمعة الشركات وعلى استقرارها المالي، وخاصة في المجالات التي تتطلب مستوى عالٍ من الامتثال القانوني. (Harvard Law Review, 2020)

- **المخاطر البيئية (Environmental Risks):** ترتبط بالتأثيرات الطبيعية على الشركة، مثل الكوارث الطبيعية كالأعاصير والزلازل والفيضانات. قد تؤدي هذه المخاطر إلى تدمير البنية التحتية للشركة أو تعطيل العمليات بشكل كامل. مع التغيرات المناخية، أصبحت هذه المخاطر أكثر تهديدًا، خاصة للشركات التي تعتمد على مواقع معينة لتشغيل أعمالها. تقرير الأمم المتحدة حول التغير المناخي، فإن الشركات في مختلف أنحاء العالم تواجه تهديدات متزايدة من الكوارث الطبيعية والتي يمكن أن تؤدي إلى خسائر اقتصادية جسيمة. (UN Climate Report, 2019)

- **المخاطر الأمنية الشخصية (Personal Security Risks):** تتعلق هذه المخاطر بسلامة وأمن العاملين في الشركة. يمكن أن تنشأ هذه المخاطر من التهديدات الجسدية مثل السرقة، الاعتداء، أو التهديدات الأمنية أثناء السفر للأعمال. كذلك، قد يتعرض الموظفون للمضايقات أو الابتزازات بسبب عملهم في الشركة. تُعتبر المخاطر الشخصية عاملاً حاسمًا في التخطيط الأمني للشركات، خاصة بالنسبة للموظفين الذين يعملون في بيئات غير مستقرة. (Global Corporate Security Council, 2020)

- **المخاطر السياسية (Political Risks):** تتعلق بالأحداث السياسية التي قد تؤثر على الشركة، مثل التغييرات في السياسات الحكومية، الانقلابات، الحروب، أو فرض عقوبات اقتصادية. تؤثر هذه المخاطر بشكل كبير على الشركات التي تعمل في بيئات سياسية غير مستقرة أو في دول تتعرض للعقوبات الدولية (لتقرير البنك الدولي، فإن المخاطر السياسية تؤثر بشكل خاص على الشركات متعددة الجنسيات التي تعتمد على استقرار البيئات السياسية لتنفيذ عملياتها التجارية. (World Bank Report, 2021)

- **المخاطر الثقافية والاجتماعية (Cultural and Social Risks):** ترتبط هذه المخاطر بالعوامل الاجتماعية والثقافية التي قد تؤثر على عمل الشركة. على سبيل المثال، قد تواجه الشركات مقاومة محلية بسبب عدم توافق منتجاتها أو خدماتها مع القيم الثقافية للمجتمعات التي تعمل فيها. كما أن التغيرات الاجتماعية مثل الاحتجاجات أو الحركات الاجتماعية قد تؤثر على سير العمل. (طبقا لدراسة من جامعة

أكسفورد حول المخاطر الاجتماعية والثقافية، تعد هذه المخاطر تهديدًا حقيقيًا للشركات التي تسعى للتوسع في أسواق جديدة دون دراسة عميقة للسياق الثقافي والاجتماعي. (Oxford University, 2018)

- **المخاطر التنظيمية (Regulatory Risks):** تتعلق بالتغيرات في اللوائح الحكومية التي تؤثر على كيفية عمل الشركات. يمكن أن تشمل هذه التغيرات في السياسات المتعلقة بالضرائب، الصحة والسلامة، أو حماية البيئة، ما قد يتطلب من الشركات تعديلات كبيرة في عملياتها. (وفقًا لتقرير منظمة التعاون الاقتصادي والتنمية (OECD)، تشكل المخاطر التنظيمية تحديًا كبيرًا للشركات العاملة في بيئات تتسم بتغيرات سريعة في اللوائح والقوانين. (OECD, 2020)

هذه الأنواع المختلفة من المخاطر تتطلب من الشركات تطبيق استراتيجيات شاملة لإدارة المخاطر والتخفيف منها. يمكن لكل نوع من هذه المخاطر أن يؤدي إلى خسائر كبيرة إذا لم يتم التعامل معه بشكل صحيح، إدارة المخاطر في الشركات السعودية تتطلب استراتيجيات فعالة وشاملة لضمان حماية الأصول، تحقيق استمرارية الأعمال، والتعامل مع التحديات المتغيرة التي تفرضها البيئة التشغيلية المحلية والدولية. مع تطور التكنولوجيا ونمو السوق السعودي، أصبح من الضروري للشركات تبني ممارسات متطورة لإدارة المخاطر من أجل مواجهة التهديدات المتزايدة. فيما يلي مجموعة لأهم الاستراتيجيات الفعالة لإدارة المخاطر في الشركات السعودية:

- تحليل المخاطر وتقييمها بشكل دوري.
- تبني التكنولوجيا الحديثة في إدارة المخاطر.
- الاستثمار في الأمن السيبراني.
- تطوير سياسات واستراتيجيات استمرارية الأعمال.
- تدريب الموظفين على إدارة المخاطر.
- تنويع مصادر التوريد والموارد.
- تعزيز الامتثال للأنظمة والقوانين المحلية والدولية.

- التواصل الفعّال وإدارة الأزمات.
- التقييم الدوري للأداء الأمني.
- بناء ثقافة إدارة المخاطر داخل الشركة.
- التعاون مع الشركاء الخارجيين.

الاستراتيجيات الفعالة لإدارة المخاطر في مجال أمن الشركات:

- تطوير خطط أمنية شاملة تغطي جميع جوانب العمليات.
- تعزيز الأمن السيبراني من خلال استخدام تقنيات حديثة ونظم حماية قوية.
- تدريب الموظفين بانتظام على أفضل الممارسات الأمنية ورفع مستوى الوعي حول المخاطر الأمنية.
- التعاون مع الجهات الحكومية والأمنية لتعزيز الأمن الشامل.
- إجراء تقييمات دورية للإجراءات الأمنية وتطويرها وفقاً لأحدث التهديدات.

التحديات الخاصة في المملكة العربية السعودية:

تواجه الشركات في السعودية تحديات فريدة مثل التهديدات السيبرانية المستمرة، والاحتياجات الأمنية الخاصة بالبنية التحتية الحرجة، والامتثال للمتطلبات التنظيمية الصارمة. تعد القدرة على التكيف مع التغيرات السريعة في البيئة الأمنية أمرًا بالغ الأهمية لضمان استمرارية الأعمال. تتطلب إدارة المخاطر والتخفيف منها في مجال أمن الشركات نهجًا متكاملًا يجمع بين التحليل الدقيق للمخاطر، وتطوير استراتيجيات شاملة، وتنفيذها بفعالية. إن الاستثمار في التكنولوجيا، وتدريب الموظفين، وتعزيز التعاون مع الجهات الخارجية، تعتبر من العوامل الرئيسية لنجاح استراتيجيات إدارة المخاطر في المملكة العربية السعودية. (الراشد، 2017)

نظرية إدارة المخاطر: تعد نظرية إدارة المخاطر واحدة من الركائز الأساسية في هذه الدراسة. تهدف هذه النظرية إلى التعرف على المخاطر المحتملة التي يمكن أن تواجه الشركات، وتقييم تأثيرها، وتطوير استراتيجيات للحد منها أو إدارتها بشكل فعال. تشمل هذه النظرية عدة خطوات رئيسية: (عبدالله، 2019)

- **تحديد المخاطر**: التعرف على جميع التهديدات المحتملة سواء كانت داخلية أو خارجية.

- **تحليل المخاطر**: تقييم احتمالية حدوث المخاطر وتأثيرها على الشركة.
- **تقييم المخاطر**: تحديد الأهمية النسبية لكل خطر بناءً على احتمالية حدوثه وتأثيره.
- **إدارة المخاطر**: تطوير وتنفيذ استراتيجيات للحد من تأثير المخاطر أو التخفيف منها.

نظرية الأمن السيبراني: في عصر التحول الرقمي، أصبحت نظرية الأمن السيبراني محورية في حماية البيانات والمعلومات الحساسة للشركات. تعتمد هذه النظرية على حماية الأنظمة والشبكات من الهجمات الإلكترونية من خلال:

- **التشفير:** حماية البيانات من الوصول غير المصرح به.
- **الجدران النارية:** منع الوصول غير المصرح به إلى الشبكات.
- **التدقيق الأمني:** مراجعة الأنظمة بانتظام للكشف عن الثغرات الأمنية.
- **الاستجابة** للحوادث: تطوير خطط استجابة فعالة للتعامل مع الهجمات السيبرانية.

نظرية الإدارة الاستراتيجية: تعتبر الإدارة الاستراتيجية جزءاً لا يتجزأ من إدارة المخاطر. تعتمد هذه النظرية على تطوير رؤية ورسالة واضحة للشركة، وتحليل البيئة الداخلية والخارجية لتحديد نقاط القوة والضعف، والفرص والتهديدات. تساعد هذه النظرية، وأنها خطة مخصصة توضح بالتفصيل كيفية تعامل المؤسسات مع المخاطر المختلفة، سواء بشكل استباقي أو عند وقوع الحوادث، وبذلك توفر نظرة تفصيلية لرواد الأعمال والمديرين التنفيذيين حتى يتمكنوا من اتخاذ قرارات مستنيرة، (النفيعي، 2021)

وتعد استراتيجية إدارة المخاطر جزءًا أساسيًا لأي خطة في هذا الخصوص، ومن ثم يتم تحديد هذه الاستراتيجية بعد تحديد المخاطر وتقييم احتمالية حدوثها، بالإضافة إلى التأثير الذي يمكن أن تحدثه، ومن ثم سوف يحتاج واضع الاستراتيجية إلى تحديد كيفية التعامل والنهج الذي سيتبعه لإدارة المخاطر وعلاجها، وتتمثل في: (محمد، 2020)

- **تحليل البيئة**: فهم العوامل الاقتصادية والاجتماعية والتكنولوجية والقانونية التي تؤثر على الشركة.
- **تطوير الاستراتيجيات:** وضع استراتيجيات فعالة تستند إلى تحليل البيئة لضمان تحقيق الأهداف التنظيمية.

- **التنفيذ والمتابعة**: تنفيذ الاستراتيجيات ومراقبة الأداء لضمان تحقيق النتائج المرجوة.

نظرية المرونة التنظيمية: تركز هذه النظرية على قدرة الشركات على التكيف مع التغيرات غير المتوقعة والتعامل مع الأزمات بفعالية. تساعد المرونة التنظيمية في: (الحسن، 2015)

- **التكيف السريع**: تعديل العمليات والاستراتيجيات بسرعة لمواجهة التهديدات الجديدة.
- **التعلم التنظيمي**: الاستفادة من التجارب السابقة لتحسين الاستعداد للأزمات المستقبلية.
- **التعاون الداخلي**: تعزيز التعاون بين الإدارات المختلفة لتحقيق استجابة منسقة للأزمات.

نظرية التغيير التنظيمي: توضح هذه النظرية كيفية تنفيذ التغييرات الضرورية في الهياكل والعمليات التنظيمية لضمان الأمان والاستدامة. تُشمل هذه النظرية: (الحربي، 2019)

- **التخطيط للتغيير:** وضع خطط تفصيلية للتغيير تتضمن الأهداف والاستراتيجيات والإجراءات.
- **إدارة التغيير:** التعامل مع مقاومة التغيير من خلال التواصل الفعّال وإشراك جميع أصحاب المصلحة.
- **تنفيذ التغيير**: تنفيذ الخطط بفعالية لضمان تحقيق الأهداف المرجوة:

نظرية التحليل الكمي والنوعي للمخاطر: يستخدم التحليل الكمي أدوات رياضية وإحصائية لتقييم المخاطر بناءً على البيانات التاريخية والمعطيات الحالية، بينما يعتمد التحليل النوعي على الخبرات والتقديرات الشخصية. كلا النوعين من التحليل يعتبران مهمين في: (عبدالله، 2020)

- **تقدير الاحتمالات**: استخدام النماذج الرياضية لتقدير احتمالية وقوع المخاطر.
- **تقييم التأثير**: تحليل الآثار المحتملة للمخاطر على العمليات التنظيمية.
- **تطوير الاستراتيجيات**: استخدام نتائج التحليل لتطوير استراتيجيات فعالة لإدارة المخاطر.

نظرية حوكمة الشركات: تركز هذه النظرية على مبادئ الشفافية والمساءلة والعدالة في إدارة الشركات. تُسهم الحوكمة الجيدة:

- **تعزيز الثقة**: بناء الثقة بين المستثمرين وأصحاب المصلحة من خلال ضمان النزاهة والشفافية.
- **الحد من المخاطر:** وضع سياسات وإجراءات قوية للحد من المخاطر المحتملة.

- **تحسين الأداء**: تحسين الأداء التنظيمي من خلال توفير بيئة عمل آمنة ومستقرة.

نظرية العلاقات الدولية: تعتبر العلاقات الدولية جزءًا من البيئة الخارجية التي تؤثر على الشركات. تسهم هذه النظرية: (زبيدي، 2018)

- **فهم التأثيرات الخارجية:** فهم التأثيرات الجيوسياسية والاقتصادية على الشركات.
- **التكيف مع السياسات**: التكيف مع السياسات والتشريعات الدولية التي تؤثر على الأمن وإدارة المخاطر.
- **تعزيز التعاون:** تعزيز التعاون الدولي لتبادل الخبرات وأفضل الممارسات في إدارة المخاطر.

نظرية التنافسية العالمية: تركز هذه النظرية على كيفية تحقيق الشركات للميزة التنافسية في السوق العالمي من خلال الابتكار والأمان. تسهم هذه النظرية: (علي، 2020)

- **تحليل السوق**: فهم اتجاهات السوق العالمية وتحديد الفرص والتهديدات.
- **تعزيز الابتكار**: تعزيز الابتكار في المنتجات والخدمات لتحسين التنافسية.
- **تحقيق الميزة التنافسية**: استخدام استراتيجيات الأمان لإدارة المخاطر وتعزيز الميزة التنافسية.
- **تساعد الدراسة** في تقديم إطار شامل لتحليل وتطوير استراتيجيات فعالة لإدارة المخاطر في الشركات السعودية. تسهم هذه النظريات في تقديم فهم أعمق للمخاطر والتحديات التي تواجه الشركات وتوفير الحلول المبتكرة للتغلب عليها وضمان الأمن والاستدامة في بيئة الأعمال الديناميكية.

الفصل الثالث: منهجية الدراسة

المنهجية وطرق البحث

- هذه الدراسة بها نوعين من الطرق: النوعي والكمي، حيث سيتم جمع البيانات من خلال المقابلات والاستبيانات وتحليل البيانات الإحصائية.
- استخدام النهج المختلط، حيث سيتم الجمع بين البيانات الكمية والنوعية

- إجراء مقابلات متعمقة مع خبراء الأمن، مديري المخاطر، والمستشارين في الشركات السعودية للحصول على رؤى حول الاستراتيجيات الحالية والتحديات.
- توزيع استبيانات على عدد كبير من الشركات لجمع بيانات كمية حول ممارسات إدارة المخاطر وأداء الأمن.
- مراجعة الأدبيات الأكاديمية والمقالات والدراسات السابقة المتعلقة بإدارة المخاطر والأمن السيبراني.
- تحليل التقارير الصادرة عن الجهات الحكومية والمؤسسات الخاصة حول المخاطر والأمن في الشركات السعودية.
- استخدام قواعد البيانات الأكاديمية مثل Google Scholar، JSTOR، وPubMed للحصول على دراسات ومقالات ذات صلة.
- سيتم تحليل البيانات الكمية من خلال استخدام البرامج الإحصائية مثل SPSS أو Excel لتحليل البيانات الكمية المجمعة من الاستبيانات. وسيتم استخدام الإحصاءات الوصفية (مثل المتوسطات والانحرافات المعيارية) والإحصاءات الاستدلالية (مثل التحليل التبايني والانحدار) لفحص العلاقات بين المتغيرات المختلفة.
- تحليل البيانات النوعية: تحليل البيانات النوعية المجمعة من المقابلات باستخدام تقنيات التحليل الموضوعي (Thematic Analysis) لتحديد الأنماط والموضوعات الرئيسية المتعلقة بإدارة المخاطر والأمن.

أدوات الدراسة

- **تحديد العينة**: اختيار عينة ممثلة من الخبراء والمديرين بناءً على معايير محددة مثل الخبرة والموقع الجغرافي.
- **إعداد دليل المقابلة**: تطوير قائمة بالأسئلة المفتوحة والمركزة على محاور الدراسة مثل التحديات والفرص في إدارة المخاطر.
- **إجراء المقابلات**: تنظيم مقابلات فردية وجماعية، إما وجهاً لوجه أو عبر الإنترنت، وتسجيل الإجابات بموافقة المشاركين.

- **تحليل البيانات**: تحليل الإجابات باستخدام التحليل الموضوعي لتحديد الأنماط والأفكار الرئيسية.
- **تصميم الاستبيان**: تطوير استبيان يحتوي على أسئلة مغلقة ومفتوحة تغطي محاور الدراسة مثل استراتيجيات إدارة المخاطر والتدابير الأمنية، وهذا من خلال:
  - **اختبار تجريبي:** إجراء اختبار تجريبي للاستبيان على عينة صغيرة لتحسين الأسئلة وضمان وضوحها.
  - **توزيع الاستبيان**: إرسال الاستبيانات إلى الشركات عبر البريد الإلكتروني أو من خلال الزيارات الميدانية.
- **جمع البيانات**: تجميع الاستبيانات المعبأة وتحليلها باستخدام البرامج الإحصائية.
- **جمع الوثائق**: جمع وتحليل الأدبيات الأكاديمية، التقارير الرسمية، والأبحاث السابقة المتعلقة بإدارة المخاطر والأمن السيبراني.
- **تحليل الوثائق:** استخدام تحليل المحتوى لاستخلاص المعلومات الرئيسية والأنماط ذات الصلة بالدراسة.
- **تحديد المواقع**: اختيار شركات محددة بناءً على تنوع الأنشطة والمخاطر التي تواجهها.
- **تسجيل الملاحظات**: مراقبة الإجراءات الأمنية وتسجيل الملاحظات بشكل منظم.
- **تحليل الملاحظات**: تحليل الملاحظات لاستخلاص النقاط القوية والضعيفة في الممارسات الأمنية.
- **التحليل الإحصائي:** ترميز وتنظيم البيانات في جداول إحصائية. استخدام برامج مثل Excel لإجراء التحليلات الإحصائية الوصفية والاستدلالية. تفسير النتائج الإحصائية لاستخلاص الاستنتاجات والتوصيات.

مجتمع البحث

يمثل مجتمع البحث الشركات السعودية التي تعتمد أنظمة إدارة المخاطر والأمن السيبراني. يمكن أن يشمل ذلك:

- شركات من مختلف القطاعات مثل: البنوك، الطاقة، التعليم، التكنولوجيا، والقطاعات الحكومية.
- المسؤولون والخبراء في مجال إدارة المخاطر والأمن السيبراني داخل هذه الشركات.

- الجهات التنظيمية* مثل الهيئة الوطنية للأمن السيبراني (NCA) في السعودية.

وبناءً على هذا المجتمع، يتم اختيار العينة التي تُستخدم لجمع البيانات بهدف دراسة وتحليل الاستراتيجيات المتبعة في إدارة المخاطر وتحسين الأمن السيبراني.

حدود الدراسة

- **أولاً: الحدود الموضوعية:** تركز الدراسة على استراتيجيات إدارة المخاطر والتخفيف منها في مجال أمن الشركات. تشمل الموضوعات الرئيسية التي سيتم تناولها: تحليل المخاطر، استراتيجيات إدارة المخاطر، الأمن السيبراني، التدريب والتوعية، التكنولوجيا. لا تشمل الدراسة الشركات التي لا تواجه مخاطر أمنية عالية أو تلك التي تعمل في قطاعات غير متعلقة بالأمن السيبراني بشكل مباشر.
- **ثانياً: الحدود المكانية:** تشمل الدراسة على الشركات والمؤسسات التي تعمل في المملكة العربية السعودية، اختيار عينة متنوعة من الشركات تشمل مختلف القطاعات (مثل التكنولوجيا، المالية، الصناعة، والخدمات). تغطي الدراسة المناطق الرئيسية في المملكة مثل الرياض، جدة، الدمام، ومكة المكرمة لضمان تنوع الجغرافيا وتغطية الشركات في مختلف البيئات الاقتصادية.
- **ثالثاً: الحدود الزمانية:** تمتد فترة جمع البيانات والتحليل على مدى شهر، من 9/6/2024 إلى 10/7/2024، وستراعي الدراسة التغيرات الموسمية والاقتصادية التي قد تؤثر على إدارة المخاطر والأمن السيبراني في الشركات.

الفصل الرابع

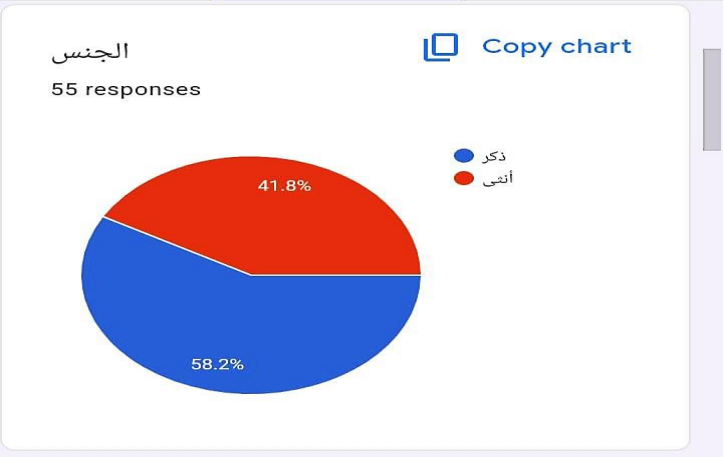
النتائج والتوصيات

تعد إدارة المخاطر جزءاً أساسياً من نجاح أي منظمة، خاصة في مجال أمن الشركات، حيث تواجه المؤسسات في المملكة العربية السعودية تحديات متزايدة تتعلق بالمخاطر الأمنية في ظل التحولات الاقتصادية والتكنولوجية السريعة. تأتي هذه التحديات في سياق سعي المملكة لتحقيق رؤيتها الطموحة 2030 التي تتضمن بناء اقتصاد رقمي وتنمية قطاعات متعددة، مما يستدعي تعزيز الاستراتيجيات الفعالة لإدارة المخاطر الأمنية والتخفيف منها.

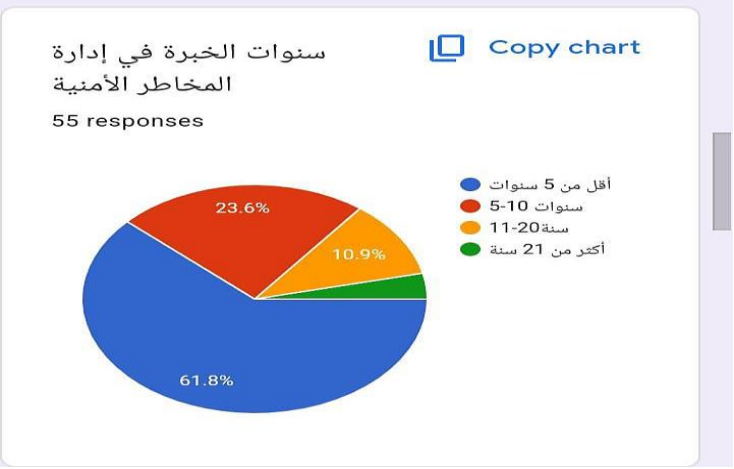
International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (3), No. (10)
IJFAES
October 2024
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (3)، العدد (10)

تحليل البيانات

تم عمل استبيان وطرح بعض الأسئلة التي تتعلق بجانب استراتيجيات إدارة المخاطر والتخفيف منها في مجال أمن الشركات بالمملكة العربية السعودية، حيث تم الاعتماد على أسلوب الاستقصاء كأداة لجمع البيانات، واختيار فروضها ومعرفة المتغيرات المراد اختبارها وقياسها، وتم ذلك من خلال استبانة صممت معتمدة على الدراسات والمراجع السابقة ذات العلاقة، وجمعها من العينة المختارة من مجتمع الدراسة.

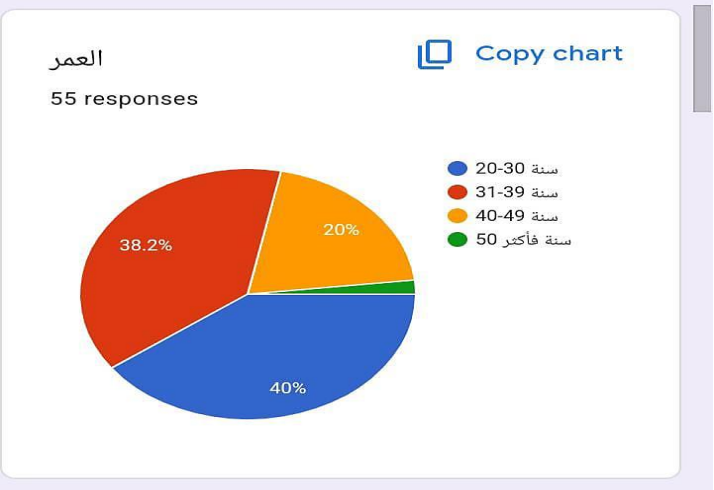


شكل (1): الخصائص الديموغرافية – الجنس-

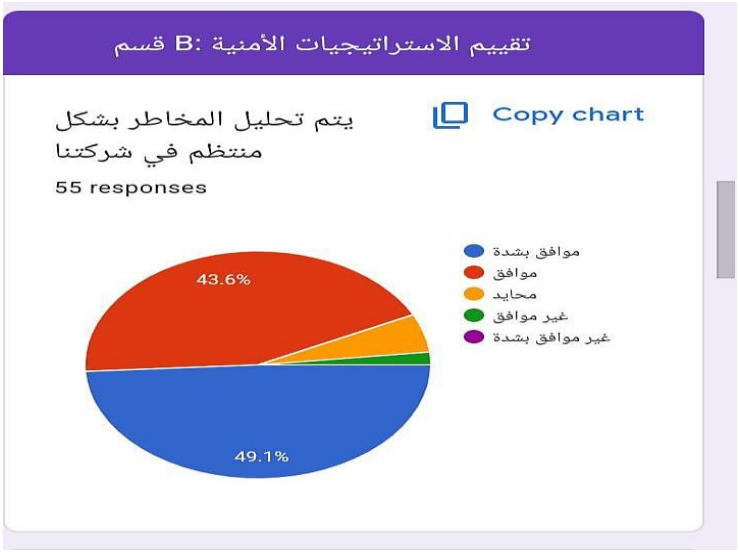


شكل (2): الخصائص الديموغرافية – العمر

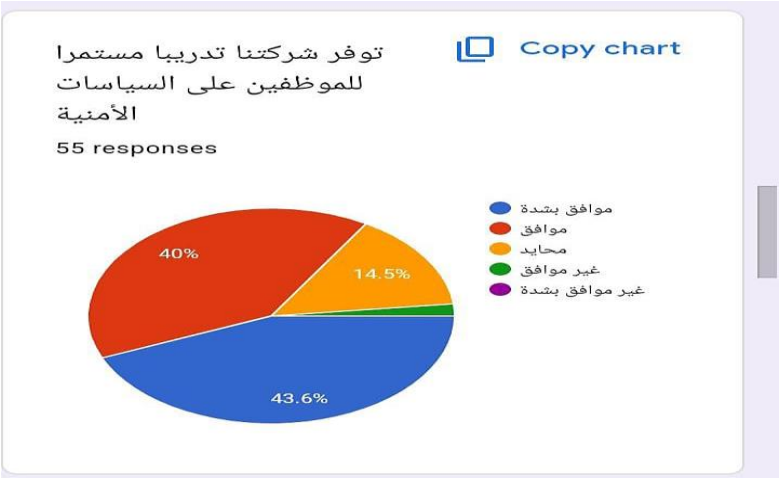
International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (3), No. (10)
IJFAES
October 2024
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (3)، العدد (10)



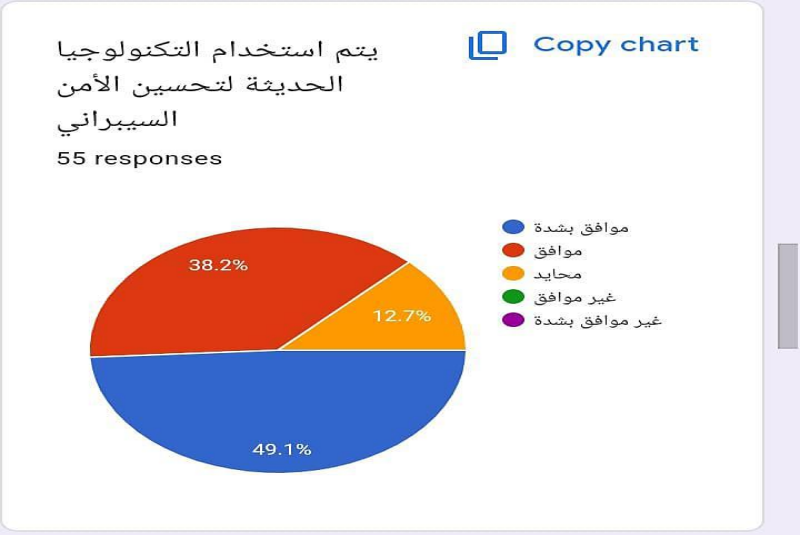
شكل (3): سنوات الخبرة في إدارة المخاطر الأمنية



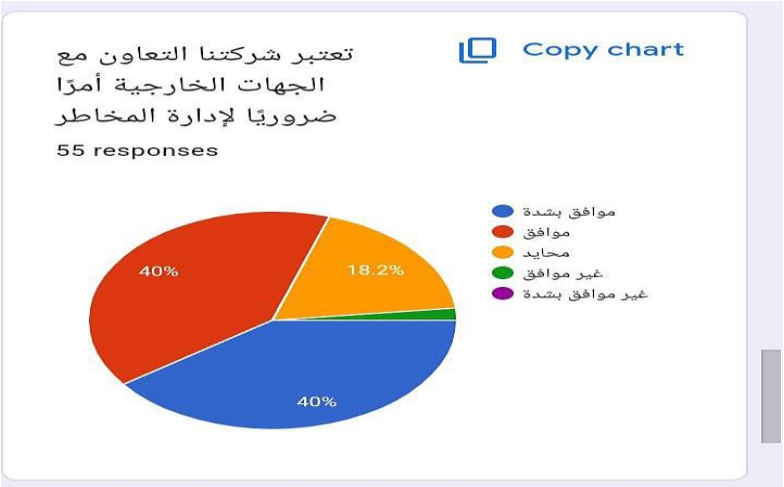
شكل (4): استبيان حول تحليل المخاطر بشكل منتظم في شركتنا



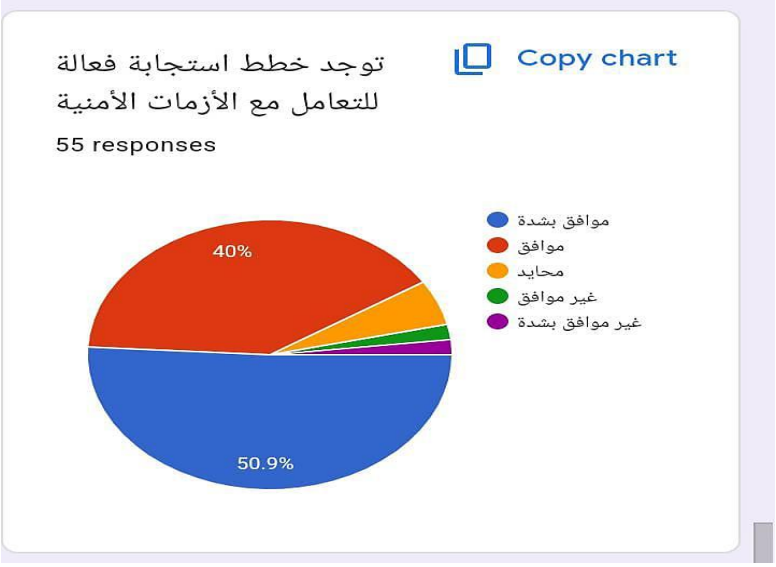
شكل (5): استبيان حول توفير الشركة لتدريب مستمر للموظفين على السياسات الأمنية



شكل (6): نسب استخدام التكنولوجيا الحديثة لتحسين الأمن السيبراني



شكل (7): نسب حول اعتبار التعاون في الشركة مع الجهات الخارجية أمر ضروري لإدارة المخاطر



شكل (8): نسب خطط الاستجابة الفعالة للتعامل مع الأزمات الأمنية

International Journal of Financial, Administrative, and Economic Sciences (IJFAES)
Vol. (3), No. (10)
IJFAES
October 2024
المجلة الدولية للعلوم المالية والإدارية والاقتصادية
الإصدار (3)، العدد (10)

شكل (9): ملاحظات حول استراتيجيات إدارة المخاطر الأمنية في الشركات

شكل (10): التحسينات المقترحة لتعزيز استراتيجيات الأمن في الشركة

شكل (11): أهم التحديات التي تواجه الشركة في إدارة المخاطر الأمنية

النتائج

من خلال الاستبيان حول الاستراتيجيات الفعالة لإدارة المخاطر والتخفيف منها في مجال أمن الشركات في السعودية، يمكننا استخلاص هذه الملاحظات الديموغرافية الهامة:

كانت نسبة المشاركين الذكور 58.2%، بينما كانت نسبة الإناث 41.8%*، مما يظهر تقارباً معقولاً في تمثيل الجنسين.

- الفئة 20-30 سنة: تشكل النسبة الأكبر بواقع 40%.
- الفئة 31-39 سنة: تمثل 38.2%، وهي قريبة من النسبة الأولى.
- الفئة 40-49 سنة: انخفضت النسبة إلى 20%.
- الفئة 50 سنة فأكثر: كانت نسبتها ضئيلة جداً، مما يعكس أن المشاركين الأكبر سناً كانوا أقل تمثيلاً.

- **سنوات الخبرة في إدارة المخاطر الأمنية:**

نتائج الاستبيان:

- أقل من 5 سنوات: 61.8%.

- 5-10 سنوات: 23.6%.
- 11-20 سنة: 10.9%.
- أكثر من 21 سنة: نسبة ضئيلة جدًا.

تظهر النتائج أن معظم المشاركين (61.8%) لديهم خبرة أقل من 5 سنوات في إدارة المخاطر الأمنية. هذا قد يشير إلى وجود مستوى منخفض من الخبرة المؤسسية في هذا المجال، مما قد يؤثر على فعالية استراتيجيات إدارة المخاطر في الشركة. من المهم أن تُعزّز الشركة من برامج التدريب والتطوير لضمان تحسين كفاءة العاملين في هذا المجال. ومع ذلك، فإن وجود 23.6% من المشاركين يمتلكون خبرة تتراوح بين 5-10 سنوات يمكن أن يُعتبر مؤشرًا إيجابيًا، حيث يمكن لهذه النسبة أن تسهم في نقل المعرفة للموظفين الجدد.

- **تقييم المخاطر في الشركة:**
  - موافق بشدة: 49.1%.
  - موافق: 43.6%.
  - محايد وغير موافق وغير موافق بشدة: نسب ضئيلة.

وتشير هذه النتائج إلى أن غالبية المشاركين (92.7%) يعتقدون أن تقييم المخاطر في الشركة يُدار بشكل جيد. هذا يدل على وجود ثقة قوية في إجراءات تقييم المخاطر الحالية، وهو ما يُعتبر نقطة إيجابية. ومع ذلك، يجب على الشركة الاستمرار في تعزيز الشفافية والتواصل مع الموظفين لضمان معالجة أي مخاوف قد تكون لديهم.

- **تدريب الموظفين على السياسات الأمنية:**
  - موافق بشدة: 43.6%.
  - موافق: 40%.
  - محايد: 14.5%.

تشير النتائج إلى أن 83.6% من المشاركين يرون أن الشركة توفر تدريبًا جيدًا على السياسات الأمنية. ومع ذلك، يجب النظر في نسبة الـ 14.5% المحايدة، حيث يُحتمل أن يكون هناك بعض النقص في وضوح أو

فعالية البرامج التدريبية. لذا، من المهم تحسين المحتوى التدريبي وجعله أكثر تفاعلاً لضمان استفادة الموظفين بشكل أكبر.

- **استخدام التكنولوجيا الحديثة لتحسين الأمن السيبراني:**

- موافق بشدة: 49.1%
- موافق: 38.2%
- محايد: 12.7%

تشير النتائج إلى دعم قوي لاستخدام التكنولوجيا الحديثة في تحسين الأمن السيبراني، حيث يُظهر 87.3% من المشاركين تأييدًا. يتعين على الشركة الاستثمار في أحدث التقنيات الأمنية لتعزيز حماية المعلومات وتقليل المخاطر. يُعتبر التحديث المستمر للتكنولوجيا والتدريب المناسب عليها جزءًا أساسيًا من استراتيجية الأمان الشاملة.

- **التعاون مع الجهات الخارجية:**

- موافق بشدة: 40%.
- موافق: 40%.
- محايد: 18.2%.

تظهر النتائج تأييدًا متوازنًا لفكرة التعاون مع الجهات الخارجية في إدارة المخاطر، مما يُعزز من فرص تبادل المعرفة والخبرات. يجب على الشركة استكشاف المزيد من الشراكات والتعاونات مع جهات خارجية لتعزيز استراتيجيات الأمن والمخاطر.

- **خطط الاستجابة للأزمات الأمنية:**

- موافق بشدة: 50.9%.
- موافق: 40%.
- محايد: نسب ضئيلة.

تشير النتائج إلى أن الشركة تمتلك خطط استجابة فعالة للأزمات الأمنية، حيث إن 90.9% من المشاركين يدعمون ذلك. من الضروري استمرار المراجعة والتحديث لهذه الخطط لضمان قدرتها على التعامل مع التهديدات المتغيرة.

- **الملاحظات النهائية:**

- توعية وتدريب الموظفين على البروتوكولات الأمنية.

- تعزيز الابتكار والإبداع.

- إنشاء نظام للبوابات الإلكترونية.

تظهر الملاحظات أهمية تعزيز الثقافة الأمنية داخل الشركة من خلال التوعية والتدريب. كما يُظهر الطلب على الابتكار أهمية تطوير استراتيجيات جديدة وفعالة لإدارة المخاطر.

التحسينات المقترحة:

- عدم السماح باستقبال البريد الخارجي إلا عن طريق أمن المعلومات.

- إنشاء بوابات إلكترونية.

تشير هذه الاقتراحات إلى رغبة قوية في تعزيز الرقابة الأمنية وزيادة مستويات الحماية. يُعتبر إنشاء بوابات إلكترونية خطوة استراتيجية مهمة نحو تأمين البيانات.

التحديات الرئيسية:

- التحول إلى الأنظمة الحديثة في الأمن.

- عدم فهم الخطورة بشكل صحيح.

تُظهر التحديات المشار إليها ضرورة التعليم والتدريب، حيث يُعتبر فهم المخاطر والتعامل معها جزءًا أساسيًا من تحسين استراتيجيات إدارة المخاطر الأمنية.

التوصيات

- يجب أن تعزز الشركة من ثقافة الأمان بين جميع الموظفين من خلال برامج توعية دورية. ينبغي على الإدارة العليا أن تكون نموذجًا يحتذى به في الالتزام بالأمن السيبراني، مما يشجع الموظفين على أخذ الأمور الأمنية بجدية.
- تنفيذ تقييمات دورية للمخاطر لتحليل التهديدات والضعف في النظام الأمني. يمكن أن تُساعد هذه التقييمات في تحديد المناطق التي تحتاج إلى تحسين وتحديث الاستراتيجيات بناءً على نتائجها.
- تشكيل فريق متخصص في إدارة المخاطر الأمنية يتكون من موظفين ذوي خبرة، يمكنهم مراقبة وتقييم الاستراتيجيات الحالية وتقديم توصيات لتحسين العمليات الأمنية.
- استكشاف استخدام تقنيات الذكاء الاصطناعي والتعلم الآلي لتحليل البيانات المتعلقة بالتهديدات الأمنية، مما يمكن الشركة من التنبؤ بالتهديدات المحتملة والاستجابة لها بشكل أسرع.
- وضع آليات فعالة للتواصل الداخلي لضمان أن جميع الموظفين على دراية بأحدث السياسات والإجراءات الأمنية. يمكن أن يشمل ذلك نشرات دورية أو اجتماعات شهرية حول الأمن.
- إعداد خطة لاستمرارية الأعمال تركز على كيفية الاستجابة للأزمات الأمنية. يجب أن تشمل هذه الخطة خطوات تفصيلية للتعامل مع مختلف أنواع الأزمات وتأثيرها على العمليات اليومية.
- تنظيم ورش عمل ودورات تدريبية متخصصة في مجالات محددة من الأمن السيبراني، مثل إدارة الهوية والوصول، وكيفية حماية البيانات الشخصية.
- تعزيز ثقافة الابتكار من خلال تشجيع الموظفين على تقديم أفكار جديدة وحلول مبتكرة تتعلق بالأمن السيبراني. يمكن أن يساعد ذلك في تحسين العمليات الأمنية وتبني أساليب جديدة.
- استثمار في أدوات وتقنيات الأمان مثل جدران الحماية، وأدوات كشف التسلل، والبرمجيات المضادة للفيروسات، لضمان حماية قوية ضد التهديدات.
- تعزيز الشراكات مع شركات الأمن السيبراني ومراكز البحوث لتبادل المعرفة والخبرات، مما يمكن أن يُحسن من استراتيجيات الأمان في الشركة.

- ضمان الامتثال لجميع القوانين واللوائح المتعلقة بالأمان السيبراني وحماية البيانات، وتحديث السياسات الداخلية بناءً على التغيرات في البيئة القانونية.
- إجراء تقييم دوري للأثر الناتج عن الإجراءات الأمنية المطبقة. يجب قياس فعالية هذه الإجراءات والتأكد من أنها تحقق الأهداف المرجوة دون التأثير سلبًا على الأداء.
- إدراك أن العنصر البشري يُعتبر أحد أكبر نقاط الضعف في الأمن السيبراني. يجب تقديم برامج تدريبية تركز على كيفية تجنب الأخطاء البشرية، مثل فتح الروابط الضارة أو تحميل ملفات مشبوهة.

الخاتمة

وفي ظل التطورات التكنولوجية المتسارعة وازدياد التهديدات الأمنية، أصبح من الضروري أن تعتمد الشركات في المملكة العربية السعودية استراتيجيات فعالة لإدارة المخاطر والتخفيف منها في مجال الأمن. إن الأمن السيبراني لم يعد مجرد خيار، بل أصبح ضرورة ملحة لحماية المعلومات الحساسة والموارد الاستراتيجية، حيث تتطلب بيئة الأعمال اليوم مرونة في مواجهة التهديدات المتزايدة، سواء كانت ناتجة عن هجمات إلكترونية متقدمة أو من المخاطر الداخلية الناتجة عن الموظفين. لذا، يجب على الشركات أن تتبنى نهجًا شاملًا لإدارة المخاطر، يقوم على تحليل دقيق للمخاطر، وتقييم مستمر للتهديدات، وتطبيق استراتيجيات استباقية.

تعتبر التوعية والتدريب من العناصر الأساسية في بناء ثقافة أمنية قوية داخل الشركات. فكلما زادت معرفة الموظفين بالمخاطر المحتملة، زادت قدرتهم على التصرف بفعالية في حالة حدوث أزمة. ينبغي أن تشمل البرامج التدريبية جميع المستويات، مع التركيز على أهمية الأمان الشخصي في الفضاء الرقمي، علاوة على ذلك، يجب أن تتبنى الشركات تقنيات حديثة وأدوات متقدمة لتحسين مستوى الأمن السيبراني. يعد الاستثمار في تكنولوجيا المعلومات الأمنية مثل جدران الحماية، وأنظمة كشف التسلل، والبرمجيات المضادة للفيروسات، ضروريًا لضمان حماية فعالة ضد التهديدات. كما يجب أن تستفيد الشركات من الذكاء الاصطناعي وتحليل البيانات لتحسين استجابة الأمن السيبراني وتحديد الأنماط الغير طبيعية في سلوك الشبكة.

تسهم الشراكات والتعاون مع الجهات الخارجية في تعزيز قدرات الأمن السيبراني. من خلال تبادل المعرفة والخبرات مع الشركات المتخصصة، يمكن أن تتعلم الشركات السعودية من أفضل الممارسات العالمية

وتكييفها مع بيئتها المحلية. كما أن التعاون مع الهيئات الحكومية والمؤسسات الأكاديمية يسهم في بناء نظام أمان شامل يتماشى مع رؤية المملكة 2030.

إن تطوير سياسات فعالة لإدارة الحوادث الأمنية واستجابة الطوارئ يعد جزءًا أساسيًا من استراتيجية الأمن. يجب أن تشمل هذه السياسات خطوات محددة للتعامل مع الحوادث فور حدوثها، وتوثيق كل الإجراءات المتخذة لتحليل فعالية الاستجابة بعد انتهاء الحادث.

وفي النهاية، يتطلب تحسين استراتيجيات إدارة المخاطر الأمنيّة وجود نهج شامل يشمل جميع جوانب الأعمال، بدءًا من الإدارة العليا وصولًا إلى الموظفين في الخطوط الأمامية. يجب أن تُعطى الأولوية لخلق ثقافة أمنية قوية تقوم على الشفافية والتواصل الفعّال بين جميع الأطراف المعنية. من خلال تطبيق استراتيجيات شاملة ومتكاملة، يمكن للشركات في المملكة العربية السعودية أن تُعزز من قدرتها على التكيف مع التهديدات المتغيرة وتكون في وضع أفضل لحماية بياناتها وأصولها الاستراتيجية، بالتالي، فإن تطوير استراتيجيات فعالة لإدارة المخاطر والتخفيف منها لا يُعتبر فقط وسيلة لحماية الأعمال، بل هو استثمار في مستقبل الشركات واستدامتها. لذا، ينبغي أن تُولي الشركات اهتمامًا خاصًا لإدارة المخاطر الأمنية كجزء لا يتجزأ من استراتيجيات النمو والابتكار، مما يسهم في تحقيق النجاح في عصر تتزايد فيه المخاطر والتحديات.

المراجع

أولاً: المراجع العربية

- النسور، بلال هاشم، (2020)، مقترح لتطبيق أبعاد حوكمة الشركات في تعزيز نجاح المشروع في مجموعة شركات المناصير، دراسة تطبيقية تحليلية، مجلة المثقال للعلوم الاقتصادية والإدارية، مج6، ع1.
- محمد، إياد طاهر، وسعيد، هشام مسلم (2020)، إدارة المخاطر وانعكاسها على جودة خدمة البلدية، دراسة استطلاعية لآراء عينة من الموظفين في مديرية مجاري صلاح الدين، مجلة تكريت للعلوم الإدارية والاقتصادية.
- الغامدي، عبدالله، 2020، إدارة المخاطر في الشركات: أفضل الممارسات في السعودية، مجلة الإدارة العامة للنشر، ط1، ص: 56-85.
- المطيري، منال، (2020)، العوامل المساهمة في نجاح المشاريع الصغيرة التي تمتلكها المرأة السعودية، كجلة الخدمة الاجتماعية، ع2.

- موسى، شقيري نوري، نور، محمود إبراهيم، الحداد، (2012)، إدارة المخاطر، دار المسيرة للنشر والتوزيع.
- القحطاني، مروان، 2019، تقييم فعالية سياسات الأمن السيبراني في الشركات السعودية، المجلة العربية للأمن السيبراني للنشر والتوزيع، ط2، ص: 141.
- الزهراني، علي، 2019، تحليل المخاطر السيبرانية وتأثيرها على الشركات في السعودية، دار المجلة العربية، ط2، ص:96-102.
- سليمان، عبدالله، (2022)، أثر إدارة المخاطر في مرونة سلسلة التوريد، الدور المعدل للتمكين في شركة البوتاس العربية (رسالة دكتوراه غير منشورة)، جامعة الإسلامية العالمية، عمان.
- الدوسري، مريم، 2019، أمن المعلومات وإدارة المخاطر في الشركات السعودية، دار الجامعة للنشر، ط1، ص:36-40.
- عبد الكريم، روان، (2018)، التوجيهات الاستراتيجية وأثرها في نجاح المشاريع، الدور الوسيط لرأس المال الفكري، دراسة ميدانية في مركز الملك عبدالله الثاني للتصميم والتطوير (رسالة دكتوراه غير منشورة)، جامعة العلوم الاسلامية العالمية، عمان.
- العتيبي، ماجد، 2018، تقييم سياسات الأمن في الشركات السعودية: دراسة حالة، دار المجلة العلمية، ط3، ص:58.
- الصالح، محمد، 2018، استراتيجيات إدارة المخاطر في الشركات السعودية: دراسة تحليلية، دار المنظومة للنشر والتوزيع، ط2، ص:106.
- طاهر، محمد، (2020)، تأثير إدارة المخاطر الفاعلة في نجاح المشروعات، دارسة تطبيقية في عينة من مشروعات البناء والتشييد الحكومية والخاصة في محافظة البصرة، مجلة دراسات إدارية، مج13، ع27.
- الشمري، فاطمة، 2017، إدارة المخاطر في الشركات السعودية: نماذج وتطبيقات، مجلة الإدارة العامة، ط1، ص:60-67.

- الشمري، عبد الرحمن، 2016، إدارة المخاطر وأمن المعلومات في الشركات السعودية، دار الثقافة للنشر والتوزيع، ط1، ص:85-93.
- العتيبي، خالد، 2021، تحديات الأمن السيبراني في الشركات السعودية: استراتيجيات وحلول، المجلة السعودية للإدارة، ط1، ص:108.
- القحطاني، سارة، 2021، استراتيجيات الأمن السيبراني للشركات السعودية: دراسة ميدانية، دار المجلة السعودية للأبحاث العلمية، ط1، ص:204-219.
- العبدلي، خالد، 2020، إدارة الأزمات في الشركات، مكتبة الأمل بالدمام، ط4، ص: 85
- الحربي، راشد، 2019، إدارة المخاطر التشغيلية في المؤسسات، دار المنارة بالرياض، ط1، ص: 131-139.
- الشدادي، علي، 2017، إدارة المخاطر الأمنية في الشركات العربية، جامعة الملك سعود، مناقشة التحديات التي تواجه الشركات العربية في مجال إدارة المخاطر الأمنية، واقتراح حلول لها، ص: 117-123.
- العمري، سالم، 2021، إدارة المخاطر المالية، دار الأندلس بجدة، ط2، ص:116.
- المطيري، ناصر. 2018، إدارة المخاطر في القطاع الصحي، دار الأفق بالمدينة المنورة، ط2، ص:115-123.
- العتيبي، خالد،2018 تأثير التكنولوجيا الحديثة على أمن المعلومات في الشركات الخليجية، جامعة الكويت، كيف يمكن للتكنولوجيا الحديثة أن تعزز أمن المعلومات في الشركات الخليجية، ص: 97.
- الجهني، فهد، 2017، إدارة المخاطر البيئية، دار الفكر بالطائف، ط1، ص:49-55.
- العتيبي، محمد. 2016، إدارة المخاطر في المشاريع الصغيرة، دار الشروق بالرياض، ط3، ص:142.
- السليمان، فهد، 2019، التحول الرقمي وأثره على الأمن السيبراني في المملكة العربية السعودية، جامعة الملك عبد العزيز، تأثير التحول الرقمي السريع في المملكة، ص: 204-210.

- السبيعي، نواف، 2019، استراتيجيات التخفيف من المخاطر في التعليم، دار الهداية بالرياض، ط1، ص:50-62.
- الزبيدي، حسن. 2018، إدارة المخاطر في القطاع الصناعي، دار العلوم، جدة، ط2، ص:145-158.
- النفيعي، محمد. 2021، استراتيجيات التخفيف من المخاطر في النقل، دار المسيرة، الرياض، ط1، ص:86-91.
- الراشد، يوسف، 2017، المخاطر في البنوك، دار اليازوري، الرياض، ط4، ص: 204.
- البقمي، خالد. 2019، إدارة المخاطر في قطاع العقارات، دار الأفق، جدة، ط2، ص:49-58.
- العمرو، عبد الله، 2020، إدارة المخاطر في الشركات الناشئة، دار التقدم، مكة المكرمة، ط2، ص: 110-129.
- الحسن، علي، 2015، إدارة المخاطر التشغيلية في المصانع دار الفاروق، جدة، ط2، ص:77-82.
- المانع، عبدالله، 2019، تحليل مخاطر الأمن السيبراني في القطاع المالي السعودي، معهد الإدارة العامة، ط1، ص: 94.
- السعد، محمد. 2020، إدارة المخاطر في المشاريع الإنشائية، دار النشر العربي، الرياض. ط2، ص:91.
- الرافعي، سالم،2017، استراتيجيات التخفيف من المخاطر في الصناعة، دار الفكر، مكة المكرمة. ط3، ص:84-91.
- العتيبي، هالة، الأمن السيبراني وإدارة المخاطر في المؤسسات التعليمية السعودية، 2021، بجامعة الملك فيصل، البحث في التحديات الأمنية التي تواجه المؤسسات التعليمية في المملكة، ص: 87-91.
- عبد العزيز، محمد ،2016، استراتيجيات الوقاية من المخاطر في الزراعة، دار المسيرة، الطائف. ط1، ص: 60-85.
- عبد الله، حسان، 2018، إدارة المخاطر في المشاريع الإنشائية، دار الفكر، جدة. ط2، ص:112-126.
- علي، محمد، 2020، إدارة المخاطر التشغيلية في النقل، دار النور، الرياض. ط3، ص:72-78.

- عبد الله، حامد، 2017، استراتيجيات الوقاية من المخاطر في التعليم، دار الفاروق، الطائف، ط3، ص:55، 57.
- عبد العظيم، طاهر، 2019، إدارة المخاطر في الشركات، دار الفكر، الرياض، ط4، ص:90.
- الناظر، (2019)، أثر إدارة التغيير على نجاح المشروعات الحكومية الإلكترونية في المملكة العربية السعودية، المجلة الدولية للعلوم الكمبيوتر وأمن الشركات.
- محمد، سليم، (2021)، تأثير تخطيط المشروع على نجاح المشاريع الإنشائية: الدور المعدل لمستوى المخاطرة، دراسة تطبيقية في شركات مشاريع الانشاءات الأردنية (رسالة دكتوراه غير منشورة، جامعة البلقاء التطبيقية، السلط).
- العوضي، فايزة خير الله، (2018)، التسويق عبر شبكات التواصل الاجتماعي ودورها في نجاح المشروعات الصغيرة، المجلة العلمية للدراسات والبحوث المالية والإدارية، مج4، ع2.
- عودة، جهاد، (2020)، المخاطر الاستراتيجية وإدارتها، المكتب العربي للمعارف.
- علي، رباب محمد، (2015)، نظام لإدارة المشاريع البرمجية، رسالة ماجستير غير منشورة، جامعة النيلين، الخرطوم.
- عزوز، علي صلاح الدين، (2019)، استراتيجيات إدارة المخاطر في المعاملات المالية، مجلة الباحث، ع7.
- https://www.arrajol.com/content/324706/%D8%A5%D8%AF%D8%A7%D8%B1%D8%A9-%D9%88%D8%A3%D8%B9%D9%85%D8%A7%D9%84/%D8%A5%D8%AF%D8%A7%D8%B1%D8%A9-%D8%A7%D9%84%D9%85%D8%AE%D8%A7%D8%B7%D8%B1
- https://ae.linkedin.com/pulse/%D8%A5%D8%AF%D8%A7%D8%B1%D8%A9-%D8%A7%D9%84%D9%85%D8%AE%D8%A7%D8%B7%D8%B1-%D8%A7%EF%BB%B7%D9%85%D9%86%D9%8A%D8%A9-rakan-aljouid-
- https://www.ncsc.gov.bh/ar/cyberwiser/professionals/network-enterprise/cyber-risks-for-leaders.html

ثانياً: المراجع الأجنبية

- Shuaib, S. M. S. (2016). Project management performance in Saudi Arabia: An exploratory study into the constructs that bttne-/b bndcoral dissertation, University of Adelaide]. Adelaide Research & Scholarshin.
- Toor, S., and Ogunlana, S. (2018). Critical COMs of Success in Large-Scale Construction Projects: Evidence from Thailand Construction Industry. International Journal of Project Management vol. 26, issue 4.
- Via Chen, W., and Chen, T. (2017). Critical Success Factors for Construction Partnering in Taiwan. International Journal of Project Management vol. 25, issue 5.
- Zuo, J., Zhao, X., Nguyen, Q. B. M., Ma, T., & Gao, S. (2018). Soft skills of construction project management professional and project success factors: A structural equation model. Engineering, Construction and Architectural Management, 25(3 ,(https:/doi.org/10.1108/ECAM- -2016-0016.

  htp://www.constructionukraine.comindex.php?item=free articles&i d_form-316
- Ahadzie, D., Proverbs, D., and Olomolaiye, P. (2018). Critical success criteria for mass housing building projects in developing countries. International Journal of Project Management. 26. (issue 6).
- Al-Arifi, Osama Abbas Ahmed, and Al-Harafsha, Malik Ibrahim Raji. (2019). the impact of international standards for project evaluation on the success of projects in Jordanian construction engineering companies (unpublished master's thesis.
- AlBalawi, Reem bint Hamdan bin Hamed, and Gihaith. Nirvana Abdul Rahman Sayed. (2022). the impact of applying Municipal and Rural Affairs and Housing in the city of Riyadh. Journal of Reading and Knowledge, Retrieved from htp://search.mandumah.com/Record/1324258.
- Al-Hiyari, 2017. Exploring Total Quality Management Practices and Their Impact on the Success of Construction Projects in Ayla Oasis Companies in Jordan. Journal of Construction Engineering and Management, 143(3), 04017006 ·https://doi.org/ 10.1061/(ASCE)CO.1943-7862.000 1260.

- Ali, Ahmed Ali Attia, and Abu Hussein, Al-Harith Muhammad Musa. (2018). the impact of supply chain integration on University, Amman. Retrieved from bttesllеataement (onpublished master's thesis). Amman Arab.
- Ayers, John Cerm, & Hutchins, Greg (2019). Project risk management. CERM Academy.
- Bond-Barnard, T. J., Fletcher, L., & Steyn, H. (2018). Linking trust and collaboration in project teams to project management success. International Journal of Managing Projects in Business, 11(2), 432-457.

  https://doi.org/10.11081JMPB-06-2017-
- D. and Robinson, L. (2023). Client versus Contractor Perspectives on Project Success Criteria. International Journal of Project Management 23 (2023).
- Bt Mazri, I. A., (2023). Critical Success Factors for Construction. Organisation. Project report submitted in partial fulfillment of the requirement for the award of the degree of Master of Science (Construction Management), University Teknologi Malaysia.
- asani, S., Shah, S. L., Chen, T, Funnell, J., & Pollard, R. W. (2015). Monitoring safety of process operations using industrial workflows. IFAC-PapersOnLine.
- Fraser-Arnott, M. (2018). Combining Project Management and Change Management for Project Success in Libraries. In Project Management in the Library Workplace (Advances in Library Administration and Organization, Vol. 38, pp. 167-
- (186Emerald Publishing Limited. https://doi.org/10.1108/S0732-067 120180000038009
- Frefer, A. A., Mahmoud, M., Haleema, H., & Almamlook, R. (2018). success criteria and critical success factors in project management. Industrial engineering management.
- ISO 27001 (2018): International Organization for Standardization. ISO/IEC 27001:2018 Information technology, Security techniques, Information security management systems, Requirements.
- McKinsey & Company (2021): McKinsey Global Institute. "Cybersecurity in a New Digital Era: Risks and Solutions." McKinsey & Company.

- NIST (2020): National Institute of Standards and Technology. "NIST Cybersecurity Framework Version 1.1." U.S. Department of Commerce.
- PwC (2020): PricewaterhouseCoopers. "Global Cybersecurity Survey: Addressing the Evolving Threat Landscape." PwC Global Reports.
- Gartner (2021): Gartner. "Top Cybersecurity Trends and Predictions for 2021." Gartner Reports.
- Deloitte (2020): Deloitte. "Crisis Management and Business Continuity Planning: Strategies for Resilience." Deloitte Insights.
- Oxford University (2019): Oxford University. "Risk Management and Employee Training for Cybersecurity." Oxford Cybersecurity Program.
- IRM (2020): Institute of Risk Management. "Risk Insurance and Financial Protection: A Comprehensive Overview." IRM Reports.
- NCA (2021): National Cybersecurity Authority (Saudi Arabia). "Cybersecurity Framework and Compliance Guidelines." National Cybersecurity Authority Reports.
- Harvard Business Review (2020): Harvard Business Review. "Effective Crisis Management in Cybersecurity Breaches." Harvard Business Review.
- ENISA (2020): European Union Agency for Cybersecurity (ENISA). "Collaborating with External Agencies in Cybersecurity." ENISA Annual Report.
- Stanford University (2019): Stanford University. "The Role of Communication in Cyber Crisis Management." Stanford Cybersecurity Research Center.
- PMI (2019): Project Management Institute. "Risk Management Culture in Modern Enterprises." PMI Research Reports.
- International Risk Management (IRM). (2018). Risk Management in the 21st Century.
- International Corporate Security Association (ICSA). (2020). Corporate Security Strategies.
- Porter, M. E. (1996). What is Strategy? Harvard Business Review.

- National Institute of Standards and Technology (NIST). (2012). Framework for Improving Critical Infrastructure Cybersecurity.
- International Organization for Standardization (ISO). (2018). ISO 31000: Risk Management Guidelines.
- European Union Agency for Cybersecurity (ENISA). (2019). Cyber Threat Landscape Report.
- Center for Internet Security (CIS). (2019). CIS Security Benchmarks.
- National Security Agency (NSA). (2017). Contingency Planning Guide.