ROLE OF INFORMATION MANAGEMENT IN ACHIEVING CYBER SECURITY IN THE ORGANIZATION: A FIELD STUDY ON THE MUNICIPALITY OF JEDDAH

Mohammed Yousef Al-Montashari [a], Dr. Uthman M. Ageeli [b]

[a,b] King Abdulaziz University - Department of Information Science

ABSTRACT : This study aimed at identifying the role of information management in achieving cyber security in Jeddah municipality, through identifying the cybersecurity threats in Jeddah municipality, the requirements of information management to protect cyber space in Jeddah municipality, and put forward a strategic vision to reinforcement cybersecurity through information management, the descriptive methodology was adopted, the researcher prepared an electronic questionnaire, the sample of the study consisted of 60 employees in information technology department in Jeddah municipality, the study showed some of cyber threats in Jeddah municipality as follow: non clarity of laws and systems for using electronic information by employees, sending viruses to Jeddah municipality devices, the chances of electronic spying on Jeddah municipality tasks, the main requirements of information management to protect cyber space in Jeddah municipality was: the assurance of information reliability, information backup, monitoring the breakthroughs for Jeddah municipality, and held training courses for employees about cyber threats, the strategic vision based on the following items: getting help from experienced to develop means of protection, Partnering with parties interested in cybersecurity, raising awareness through courses and workshops dedicated for security aspects. The results showed that there were no statistically significant differences between the respondents for the axes of the questionnaire.

In light of these results, the researcher proposed some recommendations to conduct studies to identify the level of applying information management in governmental organizations, and private organizations, to identify the obstacles of applying information management in governmental and private organizations.

دور إدارة المعلومات في تحقيق الامن السيبراني في المنظمة : دراسة ميدانية على أمانة محافظة جدة

محمد يوسف المنتشري[1]، د. عثمان موسى عقيلي[2]

جامعة الملك عبد العزيز– قسم علم المعلومات

الملخص

هدفت الدراسة إلى تعرف دور إدارة المعلومات في تحقيق الأمن السيبراني في أمانة جدة، وذلك من خلال تعرف المخاطر السيبرانية في أمانة جدة، متطلبات إدارة المعلومات اللازم تطبيقها لحماية الفضاء السيبراني في أمانة جدة، ووضع تصور استراتيجي لتعزيز الأمن السيبراني من خلال إدارة المعلومات، واتبعت الدراسة المنهج الوصفي التحليلي، وأعد الباحث استبانة تم تطبيقها إلكترونياً، وتكونت عينة الدراسة من 60 موظف من العاملين في تقنية المعلومات في أمانة محافظة جدة، وأظهرت نتائج الدراسة وجود عدد من المخاطر السيبرانية في أمانة جدة ومنها: عدم وضوح القوانين والأنظمة الخاصة باستخدام المعلومات الإلكترونية للموظفين، وظاهرة إرسال الفيروسات إلى أجهزة أمانة جدة، فرص التجسس الإلكتروني على أعمال أمانة جدة، أما أهم متطلبات إدارة المعلومات اللازم تطبيقها لحماية الفضاء السيبراني في أمانة جدة فهي: التأكد من موثوقية المعلومة، النسخ الاحتياطي للمعلومات، رصد الاختراقات لأنظمة أمانة جدة، وعقد الدورات التوعوية للعاملين حول المخاطر، واستند التصور الاستراتيجي لتعزيز الأمن السيبراني من خلال إدارة المعلومات إلى العناصر التالية: الاستعانة بالخبرات لتطوير وسائل الحماية، الشراكة مع الجهات المهتمة بالأمن السيبراني، زيادة الوعي من خلال الدورات وورش العمل المتعلقة بالنواحي الأمنية، وأظهرت نتائج الدراسة عدم وجود فروق ذات دلالة إحصائية بين استجابات افراد العينة على جميع محاور الاستبانة.

في ضوء تلك النتائج، تقدم الباحث ببعض التوصيات لإجراء دراسات لمعرفة مستوى تطبيق إدارة المعلومات في المؤسسات والمنظمات الحكومية، بالإضافة إلى المؤسسات الخاصة، ومعرفة معوقات تطبيق إدارة المعلومات في المنظمات الحكومية، بالإضافة إلى المؤسسات الخاصة، وذلك في ضوء الأهمية التي تمثلها إدارة المعلومات في تحقيق الأمن السيبراني.

مقدمة

أدى التقدم الهائل والمتسارع في مجال تكنولوجيا المعلومات والاتصالات إلى تطورات طالت كافة مجالات الحياة المعاصرة، وكان لتلك التطورات العديد من الجوانب الإيجابية والتي جعلت من العالم قرية صغيرة، وأصبح من الممكن تجاوز الحدود المكانية والجغرافية وتبادل المعلومات بسرعة غير مسبوقة، وظهرت أنماط جديدة للتعلم والتجارة والتسوق والإدارة ارتبط تطبيقها بطابع إلكتروني معاصر، ومنها التعلم الإلكتروني والتسوق الإلكتروني والتجارة الإلكترونية والإدارة الإلكترونية.

وكما كان لهذا التطور العديد من الآثار الإيجابية، فقد كانت هناك مخاطر وتهديدات جديدة، ومنها ظهور طرق جديدة لارتكاب الجرائم في الفضاء السيبراني، واصبح على المجتمع بأفراده ومؤسساته الاحتياط من تلك الجرائم، وضرورة اتخاذ التدابير اللازمة في هذا المجال (الخالد، 2018)، واتخذت تلك الجرائم صور وأشكال متنوعة أهمها جرائم التعدي على البيانات المعلوماتية، واعتراض بيانات معلوماتية، والتعدي على الأنظمة المعلوماتية والولوج غير المشروع إلى نظم معلوماتية، وجرائم إعاقة عمل معلوماتي (الردفاني، 2014).

ونتيجة لهذا الخطر، فقد بادرت الدول الكبرى وعلى رأسها الولايات المتحدة الأمريكية باتخاذ الإجراءات اللازمة لمواجهة هذا الخطر، وانشأت وزارة الدفاع الأمريكية عام 2009 قيادة عسكرية مهمتها الرد على هجمات قراصنة المعلوماتية وتنفيذ عمليات في الفضاء الإلكتروني، باعتبار أن الأخطار المرتبطة بالأمن السيبراني من أخطر التحديات التي يواجهها الاقتصاد والأمن القومي في القرن الحادي والعشرين (خليفة، 2017)، وأعلنت أكثر من 130 دولة حول العالم عن تخصيص أقساماً وسيناريوهات خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني، بالإضافة إلى جهود محاربة الجرائم الإلكترونية، الاحتيال الإلكتروني، والأوجه الأخرى للمخاطر السيبرانية (نجيب، 2015).

وفي ضوء هذا الكم الهائل من المعلومات وما يرتبط بانتشارها وسهولة تداولها من مخاطر تصل إلى تهديد أمن الدول واستقرارها، فقد أصبح من الضروري وجود استراتيجية ملائمة لإدارة تلك المعلومات، وأن تتناسب هذه الاستراتيجية مع طبيعة تكنولوجيا المعلومات، كما أصبحت هناك حاجة ماسة إلى إطار عملي شامل لأمن المعلومات يتصف بهيكلة وصياغة جيدتين وسهلتي الفهم والإدراك من قبل أعضاء المنظمة (محمد، 2013)، وفي هذا السياق فقد ظهرت إدارة المعلومات كأحد الأساليب الإدارية المستحدثة في مجال الإدارة، بهدف التعامل مع المعلومات وتنظيمها وتصنيفها وحماية مصادر وقواعد المعلومات، والاستفادة منها في اتخاذ القرارات (الهواسي والبرزنجي، 2014).

ويتركز اهتمام إدارة المعلومات بضمان المداخل التي توصل إلى المعلومات، وتوفير الأمان والسرية للمعلومات ونقلها وإيصالها إلى من يحتاجها، وخزن المعلومات واسترجاعها عند الطلب، وتضمن إدارة المعلومات استخدام أدوات تكنولوجيا المعلومات لتوفير استخدام أكثر فاعلية وكفاءة لكل المعلومات المتاحة لمساعدة المجتمع أو المنظمة أو الأفراد في تحقيق أهدافهم(العيسى، 2014).

مشكلة الدراسة:

أولت حكومة المملكة العربية السعودية اهتماماً كبيراً بالأمن السيبراني، وتمثل ذلك في صدور الأمر الملكي الكريم رقم (6801) بتاريخ 1439/2/11هـ الموافق 2017/10/31م بإنشاء هيئة باسم (الهيئة الوطنية للأمن السيبراني) ترتبط بمقام خادم الحرمين الشريفين – أيده الله – والموافقة على تنظيمها، وتستهدف الهيئة الوطنية للأمن السيبراني التأسيس لصناعة وطنية في مجال الأمن السيبراني تحقق للمملكة العربية السعودية الريادة في هذا المجال، انطلاقا من رؤية المملكة "2030".

وقد ظهرت الحاجة إلى تحقيق الأمن السيبراني، في ضوء ما تتعرض له المملكة ومؤسساتها من هجمات وتهديدات عبر الفضاء السيبراني، ومنها ما أشار إليه المركز الوطني من هجمات إلكترونية تسعلا لاختراق أجهزة عدد من الجهات الحكومية، وسرقة المعلومات عن طريق فتح

المرفقات بالبريد ثم إرسالها إلى حسابات بريد إلكتروني أخرى، ووجود ثغرات إلكترونية في مواقع حكومية وصناعية حساسة، وأن بعض الشبكات الحكومية تعاني ضعفاً من قدرتها على مواجهة الاختراقات والتهديدات الإلكترونية (الخالد، 2018).

ومع الأخذ في الاعتبار الدور الهام الذي يُمكن أن تؤديه إدارة المعلومات، باعتبارها أحد الأساليب الإدارية المعاصرة، في إدارة المعلومات وحمايتها وسريتها وتأمين مشاركتها بين المستخدمين، فقد تمثلت مشكلة الدراسة في الإجابة عن السؤال الرئيس التالي:

ما دور إدارة المعلومات في تحقيق الأمن السيبراني في أمانة جدة ؟

ويتفرع منه هذه الأسئلة :

1. ما المخاطر السيبرانية في أمانة جدة ؟
2. ما متطلبات إدارة المعلومات اللازم تطبيقها في حماية الفضاء السيبراني في أمانة جدة؟
3. ما التصور الاستراتيجي لتعزيز الأمن السيبرانى من خلال إدارة المعلومات؟
4. هل توجد فروق ذات دلالة إحصائية بين استجابات افراد العينة بالنسبة لدور إدارة المعلومات في تحقيق الأمن السيبراني؟

فروض الدراسة

1. لا توجد فروق ذات دلالة إحصائية بين استجابات افراد العينة، تُعزى إلى متغير الجنس، بالنسبة لدور إدارة المعلومات في تحقيق الأمن السيبراني؟
2. لا توجد فروق ذات دلالة إحصائية بين استجابات افراد العينة، تُعزى إلى متغير عدد سنوات الخبرة ، بالنسبة لدور إدارة المعلومات في تحقيق الأمن السيبراني؟
3. لا توجد فروق ذات دلالة إحصائية بين استجابات افراد العينة، تُعزى إلى متغير المؤهل العلمي، بالنسبة لدور إدارة المعلومات في تحقيق الأمن السيبراني؟

أهداف الدراسة:

تتمثل أهداف الدراسة الحالي في ما يلى:

1. التعرف على المخاطر و واقع الامن السيبراني بأمانة جدة .
2. معرفة متطلبات إدارة المعلومات اللازم تطبيقها في حماية الفضاء السيبراني بأمانة جدة
3. وضع تصور استراتيجي من خلال إدارة المعلومات في مواجهة مخاطر الامن السيبراني .

أهمية الدراسة:

تتمثل أهمية الدارسة في ما يلى:

أولا: الأهمية النظرية: تعالج هذه الدراسة موضوع إدارة المعلومات في المؤسسات باعتباره مجالا جديدا في البحث العلمي نظرا إلى أن المعلومات بكل خصائصها وأنواعها المختلفة خاصة داخل المؤسسات وخارجها قد أصبحت في عصرنا الراهن حجر الزاوية في التسيير والإدارة والتنظيم والتخطيط الاستراتيجي في جميع أجهزة المنظمة بمختلف المؤسسات العالمية بتعدد أشكالها ووظائفها لما لها من أهمية بالغة في صناعة ودعم القرار السليم والفعال خاصة أثناء حدوث الأزمات التي تتعرض لها المؤسسات أثناء تأدية أنشطتها الإنتاجية أو الخدمية، مما جعلها الركيزة الأساسية التي تعتمد عليها الدول المتقدمة حاليا فى بناء منظوماتها المعلوماتية في جميع منشآتها، كما صارت إدارتها من قبل المنظمة لها قواعدها وضوابطها المنهجية والتطبيقية الخاصة مما جعلها وسيلة مهمة وضرورية لمواجهة الأزمات المؤسساتية ومواقفها المفاجئة.

كما تتمحور أهمية الدراسة حول مدى تأثير استخدام إدارة المعلومات في تطوير وتحسين الامن السيبراني سواء أكانت مخاطر داخلية أو مخاطر خارجية التي تواجه الأمانة لكون إدارة المعلومات أحد أهم العلوم التى تسعى لإيجاد بيئة معلوماتية آمنه وفق مبادئ وأسس علمية بحته مما يسهم في ارتقاء بالأمن المعلوماتي بالمنظمة وجودة التصدي لتلك المخاطر التي تقلل من درجة الموثوقية في بياناتها من قبل المتعاملين معها.

ثانياً: الأهمية التطبيقية: من المتوقع أن يستفيد من نتائج هذه الدراسة إدارة الامن السيبراني في أمانة جدة وهي الإدارة المعنية بهذه الدراسة حيث يقدم لها مجموعة من التوصيات التي تسهم بزيادة وضوح الرؤيا لدى مديري إدارة الامن السيبراني، وهناك جهة أخرى ستقدم لهم الدراسة إضافة وهم القائمون على إدارة المعلومات بالمنظمة من الممكن أن تفيدهم في كشف علاقة الارتباط بين إدارة المعلومات والأمن السيبرانى ، كما وتقدم الدراسة توصيات حول أفضل السبل للارتقاء والتطوير المستمر .

حدود الدراسة:

- **الحدود الموضوعية:** إدارة المعلومات و الامن السيبراني.
- **الحدود المكانية** : إدارة الامن السيبراني في أمانة جدة .
- **الحدود الزمانية** : الخطة الزمنية للدراسة خلال ثلاثة أشهر الأولى من سنة 1440 هـ

مصطلحات الدراسة :

إدارة المعلومات: هي مجموعة الإجراءات والأنشطة التي تتم على المعلومات ابتداءً من جمعها وتحليلها وتنظيمها وتخزينها واسترجاعها وحمايتها وفق سياسات وتنظيمات محددة.

الأمن السيبرانى: مجموعة الوسائل والتدابير والسياسات التي تُستخدم بهدف الحيلولة دون الوصول للمعلومات للغير المصرح لهم و حمايتها من أي عبث كان و يشمل كل ما له مساس بالتقنية.

الإطار النظري والدراسات السابقة

مفهوم إدارة المعلومات

تُعرّف إدارة المعلومات باعتبارها عملية معالجة البيانات والحصول على المعلومات وتنقيتها وتخزينها ومعالجتها وتحليلها وتفسيرها، واتخاذ ما يلزم من إجراءات خاصة بسير العمل الإداري في ضوء ما سبق من عمليات (حريم، 2003)، وتُعرف كذلك بأنها "جمع وإدارة وتوزيع المعلومات بوصفها مورداً استراتيجيا للمؤسسة، وذلك لتحقيق الكفاءة والفاعلية فيما تصدره من قرارات وما تسعى إليه من أهداف" (قنديلجي والسامرائي، 2002).

كما تمثل إدارة المعلومات مجموعة العمليات التي تشمل تحديد ما هو مطلوب من معلومات وتطويرها وتفعيل المشاركة بها وتقويمها، من أجل إضافة قيمة إلى الأعمال لينعكس ذلك في تطوير وتحسين الانتاجية وتسهم في تحقيق ميزة تنافسية مستدامة للمنظمة، أو أنها " العملية التي تتضمن أدوات تكنولوجيا المعلومات بهدف استخدام أكثر فاعلية للمعلومات المتاحة لمساعدة المجتمع، أو المنظمة، أو الأفراد في تحقيق أهدافهم" (البغدادي والعبادي، 2010).

ومن جهة أخرى فإن إدارة المعلومات لا تعني بالأنظمة أو التقنيات كما هو الحال مع نظم المعلومات أو تقنية المعلومات، إنما هي مجموعة من الأنشطة والعمليات والممارسات التي تهدف إلى تحقيق الكفاءة (الهواسي والبرزنجي، 2014)، في هذا السياق تجدر الإشارة إلى أنه كثيراً ما يرد مفهوم إدارة المعلومات في بعض الأدبيات بمفاهيم متعددة ومنها: نظم المعلومات، تقنية المعلومات، إدارة البيانات، وهندسة المعلومات، ولكن إدارة المعلومات تمثل مفهوماً أشمل من تلك المفاهيم السابقة، حيث تمثل الاستخدام الأمثل لتقنية المعلومات وهندسة النظم، وأتمتة المكاتب بهدف تنظيم وإدارة ومراقبة المعلومات الخاصة بالمنظمة (Chen, Synmann & Sewdass, 2005).

ومن المفاهيم الأخرى ذات الصلة بإدارة المعلومات مفهوم إدارة المعرفة، والتي تمثل إحدى استراتيجيات الشركات الاستثمارية والتي يرجع تاريخها إلى مفهوم الإدارة العلمية، ثم الإدارة بالأهداف، وصولاً إلى الاستراتيجيات الحديثة ومنها إدارة الجودة الشاملة، والتعليم التنظيمي حتى إدارة المعرفة، والتي تتعلق برأس المال الفكري أو الأصول غير الملموسة وطرق قياسها (العسكر، 2013).

ويتضح الاختلاف بين إدارة المعلومات وإدارة المعرفة باعتبار أن التعامل مع الأشياء والبيانات يُعد من اختصاص إدارة المعلومات، أما إدارة المعرفة فتهتم بالتعامل مع الموارد البشرية، أي أن إدارة المعلومات تتعلق بالوثائق والرسومات والتصميمات المعدة يدوياً أو بالحاسوب، وبالجداول الإلكترونية، وتهتم بتوفير المداخل إلى المعلومات وأمنها وانتقالها وتوثيقها واسترجاعها (الصادق، 2017)، أما إدارة المعرفة فتهتم بالاستثمار الأمثل لرأس المال الفكري وتحويله إلى قوة إنتاجية تسهم في تنمية أداء الفرد ورفع كفاءة المؤسسة (مسلم، 2014).

وظائف ومهام إدارة المعلومات:

تُعتبر إدارة المعلومات من الأمور شديدة الأهمية لكل مؤسسة أو منظمة من منظمات الأعمال، نظراً لقدرتها على الاستجابة لاحتياجات المؤسسة من المعلومات، اعتماداً على مدى جودة إنشاء تلك المعلومات واستخدامها وحفظها (Kooper et. al.,2015)، ويأتي الدور الأهم لإدارة المعلومات في صياغة القواعد التي تضمن المحافظة على المعلومات وتوزيعها واستخدامها في المنظمة بشكل فعال (تعلب، 2010).

وبالإضافة إلى ذلك تؤدي إدارة المعلومات العديد من الوظائف والمهام المتعلقة بالتعامل مع المعلومات ويُمكن إيجازها على النحو التالي (الهواسي والبرزنجي، 2014):

1. التأكد من وصول المعلومات لمن يحتاجها في الوقت الذي يحتاجها فيه من خلال أدوات ووسائل الوصول كالبوابات الإلكترونية والأجهزة الكفية والهواتف الذكية، وغير ذلك من وسائل اتصال.
2. تهيئة بيئة مناسبة لتشارك المعلومات بين العاملين عليها عبر أدوات المشاركة كالمنتديات والمدونات والشبكات الاجتماعية.
3. تهيئة أدوات البحث المناسبة التي تساعد الآخرين على الوصول للمعلومة أينما كانت داخل المنظمة أو حتى خارجها.
4. العمل على تحليل المعلومات المتوافرة لتساعد على تطوير العمل وتجنب المخاطر واتخاذ القرار.
5. حماية المعلومات والحفاظ على سريتها وملكيتها من خلال أنظمة وأدوات الحماية الإلكترونية كأدوات التشفير والتوقيع الإلكتروني وأنظمة إدارة السجلات.
6. أتمتة الأعمال المرتبطة بالمعلومات لتوفير الوقت والجهد اللازم لإنجازها أو إنتاجها أو عرضها.
7. المساعدة في تصنيف المعلومات وهندستها بشكل علمي اعتماداً على الاحتياجات الرئيسة للمستخدمين لها فتسهل عملية الوصول المباشر للمعلومة وقت الحاجة.
8. عرض المعلومات بالشكل الملائم لطبيعة من يحتاجها سواء عبر الويب أو الأجهزة المتنقلة وذلك باستخدام الرسوم البيانية والتقارير ونحوها.
9. تهيئة الوسائل المناسبة لجلب المعلومات وتجميعها من مصادرها المختلفة سواء الإلكترونية أو الورقية وتشذيبها وفقاً للحاجة.
10. المساعدة في وضع السياسات الملائمة لإدارة المعلومات بالشكل المطلوب وبما يضمن حمايتها وتوفرها بشكل مستمر.
11. أرشفة المعلومات لوقت طويل وحفظها بشكل آمن على أجهزة التخزين لاستعادتها عند الحاجة.
12. إدارة التغيير بتدريب العاملين على إنتاج المعلومات وعلى التعامل مع التقنيات الحديثة للوصول للمعلومة.

وتؤثر إدارة المعلومات تؤثر بشكل كبير وهام في عملية صنع القرار، وذلك من خلال تقديم المعلومات ذات الصلة بالقرار المراد اتخاذه، في صورة منظمة موجزة دقيقة وموثوقة في الوقت المناسب للأشخاص المعنيين بعملية صنع القرار، كما تضمن إدارة المعلومات متابعة تحديث تلك المعلومات حسب الظروف الطارئة على بيئة العمل، وهو ما يعني اتخاذ قرار سليم مستنير يُراعي كافة المستجدات والتطورات، وتأتي

مساهمة إدارة المعلومات في صنع القرار على المستويين التشغيلي والاستراتيجي بصورة تتفق مع الخطط والمشاريع طويلة الأمد (Touray et. al., 2013).

ومن المهام والمسؤوليات الأخرى الخاصة بعمل إدارة المعلومات (البغدادي والعبادي، 2010):

1. **وضع وإعداد أنظمة:** بهدف التأكد من توفر المعلومات بطريقة روتينية تضمن وصولها إلى من يحتاجها عند الحاجة وبالشكل المناسب، ويتم ذلك من خلال تحديد البيانات التي يحتاجها متخذو القرارات وكيفية معالجتها لتصبح ذات معنى لهم.
2. **مراقبة حالة المعلومات والتأكد من كفايتها وسلامتها:** وذلك من خلال الاحتفاظ بالمعلومات الهامة بشكل دقيق، بحيث تكلف الإدارة موظفين معينين لحصر المعلومات التي يحتاجها متخذ القرار، ومتى يحتاجها وبأي صيغة مع ضمان توفيرها بالشكل والوقت المناسبين.
3. **التطوير المستمر لأنظمة المعلومات:** وهو أمر ضروري في عصر الثورة المعلوماتية والتكنولوجية، لذا يتحتم على المنظمة متابعة التطورات والاستفادة منها للتطوير المستمر لأنظمتها، من خلال تطوير الأنظمة القائمة أو تصميم أنظمة جديدة.
4. **حماية المعلومات:** إن المعلومات المهمة والاستراتيجية التي تخص المنظمة يجب الحفاظ عليها والتعامل معها بشكل سري وفق ضوابط محددة، تشمل مجموعة الإجراءات والتدابير الوقائية التي تُستخدم للحفاظ على المعلومات وسريتها، حيث أصبحت مشكلة حماية البيانات والمعلومات والحفاظ عليها من التلاعب أو الاختراق غير المشروع موضع اهتمام إدارة المعلومات.

أهداف إدارة المعلومات:

يمكن وضع مجموعة من الأهداف التي تسعى إدارة المعلومات إلى تحقيقها وتتمثل هذه الأهداف فيما يلى (عصفور، 2005):

- ربط المنظمة مع بعضها في نظام متكامل بما يسمح بتدفق البيانات والمعلومات بين تلك النظم وبما يؤدى إلى تحقيق التنسيق بين أنشطة تلك النظم.
- المساعدة في ربط أهداف النظم الفرعية للمنظمة بالهدف العام للمنظمة وبالتالي المساهمة في تحقيق هذا الهدف.
- المساعدة والمساندة في عملية صنع واتخاذ القرار في جميع المستويات التنظيمية من خلال توفير التقارير التي تضمن المعلومات اللازمة لتلك القرارات في الوقت المناسب.
- توفير المعلومات اللازمة لأغراض التخطيط والرقابة في المكان والوقت والشكل المناسب.
- الرقابة على عملية تداول البيانات والمعلومات وحفظها.
- تحسين أداء الجهات المعنية من خلال إنتاج التقارير عن العمليات الروتينية للمنظمة بدقة، وتحديث البيانات والمعلومات، والتنبؤ بالمشاكل التي يمكن التعرض لها والتي من أهمها الأمن السيبرانى.
- تطوير أداء المنظمات من خلال ما تنتجه من معلومات مرتدة عن تنفيذ الخطط والمشروعات.

مفهوم الأمن السيبرانى:

يُعد مفهوم الأمن السيبراني أو أمن الفضاء الإلكتروني من المفاهيم الحديثة، والتي ظهرت في سياق ثورة تكنولوجيا المعلومات والاتصالات المعاصرة، وتشير كلمة الأمن في هذا المجال إلى إجراءات الحماية ضد التعرض للأعمال العدائية والاستخدام السيئ لتكنولوجيا الاتصال والمعلومات (عبد الصادق، 2017).

وعرف الاتحاد الدولي للاتصالات في تقريره الصادر بعنوان حول "اتجاهات الاصلاح في الاتصالات للعام 2010-2011" الأمن السيبراني باعتباره مجموع الأدوات والسياسات ومفاهيم الأمن وضوابط الأمن والمبادئ التوجيهية ونهج إدارة المخاطر، والإجراءات والتدريب وأفضل الممارسات، وآليات الضمان والتقنيات التي يُمكن استخدامها في حماية البيئة السيبرانية، وتشمل أصول المؤسسات ومستخدمي

أجهزة الحوسبة الموصولة بشبكة الانترنت، والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات ومجموع المعلومات المنقولة أو المحفوظة في البيئة السيبرانية.

ويعرفه "فون سولمس" (Von Solms, 2015) بأنه اتخاذ جميع التدابير اللازمة لحماية الأفراد من أخطار الفضاء الإلكتروني.

ويرى "كانونجيا وماندارينو" (Canongia and Mandarino (2014 أن الأمن السيبراني هو "فن ضمان ووجود واستمرارية مجتمع المعلومات، وضمان وحماية الفضاء الإلكتروني، بما يشمل المعلومات والأصول والبنية التحتية الحيوية"

كما يُعرف الامن السيبراني بانه النشاط الذي يؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن امكانات الحد من الخسائر والاضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح اعادة الوضع الى ما كان عليه، بأسرع وقت ممكن، بحيث لا تتوقف عجلة الانتاج، وبحيث، لا تتحول الاضرار الى خسائر دائمة (جبور، 2012).

ويشمل الأمن السيبراني الحد من مخاطر الهجمات والبرمجيات الخبيثة والفيروسات والتي تستهدف البرامج وأجهزة الحاسوب وشبكات المعلومات والاتصالات، واستخدام الأدوات الخاصة بالكشف عن عمليات اختراق الشبكات وإيقاف الفيروسات، وفرض نظم المصادقة وتمكين الاتصالات المشفرة، وعلى هذا يُعرف الأمن السيبراني بأنه "عملية تنظيم وتجميع الموارد والعمليات والهياكل التي تُمكن الفضاء السيبراني من إيقاف عمليات الاختراق بصورها المختلفة، والتي تتم بصورة غير صحيحة قانونية" (Craig, Daikun & Purse, 2014)

أهمية إدارة الامن السيبراني :

تأتي أهمية الأمن السيبراني في عالم اليوم بصورة لا تقل عن أهمية الأمن القومي لأي دولة، حيث ظهرت الجرائم الإلكترونية، واستخدام الفضاء الإلكتروني في القيام بحروب غير تقليدية عبر هجمات الإرهاب الإلكتروني وإطلاق فيروسات الحاسب والتجسس الإلكتروني والاختراق المباشر لشبكات المعلومات، ولم تعد أشكال الخطر التي تهدد المحتوى المعلوماتي والمجتمعي المشترك مقصورة على الأشكال التقليدية، بل أصبح لها أوجه رقمية إلكترونية غير مسبوقة في شمولها وعمقها واتساع نطاق تغطيتها، وفداحة أضرارها وتعقد آلياتها وتواصل هجماتها وتتضمن إفساد وتعطيل إتاحة المعلومات مثل المعلومات العسكرية والأمنية والاقتصادية والمحتوى الفكري والسياسي والاجتماعي والعلمي (عبد الصادق، 2017).

وللأمن السيبراني بعد اجتماعي كبير في عالم اليوم، الذي يشهد استخداماً متزايداً لمواقع التواصل الاجتماعي من قبل شرائح كبيرة من فئات عمرية مختلفة، حيث تُستخدم تلك المواقع للتعبير عن التطلعات والطموحات الشخصية لمستخدمتها، كما تتم مشاركة الأفكار والمعلومات بين ملايين المشتركين حول العالم، وعلى هذا تشير (جبور، 2012) إلى أهمية تحقيق الامن السيبراني وضمانه، ومكافحة المحتويات غير المشروعة وغير المرغوب لما لها من تأثير سلبي أكيد، على اخلاقيات المجتمع معين، وعلى ارتفاع نسبة الممارسات الجرمية، ومن الامثلة على ذلك: الاباحية، والترويج للإتجار بالممنوعات، والدعارة، والارهاب، والتجنيد لقضايا تمس الامن والسلام الدوليين. وعليه، لا بد من بناء مجتمع مسؤول، ومدرك لمخاطر الفضاء السيبيراني، قادر على التعامل بحد ادنى من قواعد السلامة، مع ادراك للعواقب القانونية، التي يمكن ان تترتب على التصرفات، والتي تعرض سلامة الغير، وسلامة رؤوس الاموال وحركتها، للخطر.

أهداف إدارة الأمن السيبراني :

تسعى إدارة الأمن السيبراني إلى تحقيق العديد من الأهداف، والتي يُمكن إيجازها على النحو التالي (الربيعة، 2018؛ أبو شنب، 2009)

1. اتخاذ جميع التدابير اللازمة لحماية مستخدمي الانترنت من المخاطر المحتملة في مجالات استخدام الانترنت المختلفة.
2. تعزيز حماية أنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.
3. حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به لأهداف غير سليمة.

4. تعزيز حماية الشبكات وأنظمة تقنية المعلومات.
5. تعزيز وحماية سرية وخصوصية البيانات الشخصية.
6. ضمان توافر استمرارية عمل نظم المعلومات.
7. التأكد من ضمان وسلامة وصول الأشخاص المصرح لهم بالاطلاع على المعلومات.
8. التحقق من سلامة ودقة المعلومات المخزنة.

ولضمان تحقق تلك الأهداف، يجب أن تتحقق معايير الأمن الأساسية وهي: السرية أو الموثوقية Confidentiality، السلامة أو الأمانة Integrity، التوافر Availability، وتعرف تلك المعايير اختصاراً بمعاييرCIA، ويشير التوافر إلى استمرار توفر المعلومة للشخص أو الجهة التي يسمح لها المستخدم بالاطلاع عليها عند الحاجة، ويُقصد بالسلامة أي عدم التلاعب بالمعلومات أو حذفها أو تعديلها بحيث يضمن المستخدم دقة نقل ما يريد من معلومات دون تدخل اثناء النقل أو التخزين أو المعالجة، أما السرية فتعني عدم كشف المعلومات لغير أطرافها بما يوفر الخصوصية والسرية للمعلومات المتداولة على الفضاء السيبراني (Goodyear et. al.,2010)

علاقة ادارة المعلومات والامن السيبراني

تتضح العلاقة بين إدارة المعلومات والأمن السيبراني، في كل مرحلة من مراحل عمل إدارة المعلومات والتي تُعرف بدورة حياة المعلومات، وتتكون تلك الدورة من المراحل الآتية (الهواسي والبرزنجي، 2018):

1. مرحلة تجميع المعلومات من مصادرها المختلفة الإلكترونية وغير الإلكترونية.
2. مرحلة إدارة ومعالجة المعلومات.
3. مرحلة تقديم المعلومات للآخرين، وتوزيعها عبر قنوات ووسائل مختلفة كالتقارير وأدوات البحث والتنقيب والتطبيقات الإلكترونية المختلفة.
4. مرحلة الاحتفاظ بالمعلومات وتخزينها بأمان لفترات زمنية طويلة كسجلات إلكترونية أو ورقية.

وفيما يلي عرض لدور أمن المعلومات في كل مرحلة من المراحل السابقة:

أولاً تجميع المعلومات والأمن السيبراني :

تتضمن هذه المرحلة الإجراءات التالية (نصيف،2010):

1. تحديد أهم مصادر جمع المعلومات اللازمة لفاعلية اتخاذ القرارات.
2. تحديد الطرق المستخدمة في الحصول على المعلومات اللازمة لفاعلية.
3. تحديد مواصفات المعلومات اللازمة.
4. تحديد متطلبات المعلومات اللازمة.
5. تجنب المعوقات التي تواجه متخذي القرارات في الحقول على المعلومات اللازمة لفاعلية اتخاذ القرارات.

وينبغي الالتزام في هذه المرحلة بمجموعة من المعايير (برهان، 2001) وهي: التأكد من صحة المعلومات، تحديث المعلومات، توفير الحجم الضروري من المعلومات، إيجاز المعلومات وتبويبها.

وعلى هذا ترتبط هذه المرحلة بتحقق معيار السلامة Integrity، ويوضح القحطاني (2015) دور هذا المعيار لضمان الثقة في المعلومة وأنها هي المعلومة الأصلية، دون زيادة أو نقصان، ويهتم هذا المعيار بعملية "كشف" عدم سلامة المعلومة وتكاملها أكثر من اهتمامه بعملية "منع" التعديل على المعلومة أو "تصحيح" ذلك التعديل، والسبب في ذلك أن أي تعديل غير مشروع على المعلومة يجعلها غير آمنة، كما يشير الاتحاد الدولي للاتصالات (2006) إلى دور الأمن السيبراني في المراقبة الصارمة لمصادر المعلومات ومنع الفيروسات وبرامج التجسس والديدان وأحصنة طروادة التي قد تتسلل اثناء عمليات جمع المعلومات من المصادر الالكترونية المختلفة.

إدارة ومعالجة ومشاركة المعلومات بين من يحتاجها والأمن السيبراني :

تعمل هذه المرحلة على نمذجة البيانات الخام، وإعادة ترتيبها وتنظيمها بشكل يجعلها مناسبة للاستخدام المستقبلي، بغية تحقيق أغراض وأهداف معينة (نوري وجمعة، 2013).

ويتمثل دور الأمن السيبراني في هذه المرحلة بعمليتين رئيسيتين وهما تصنيف المعلومات Information Classification والتوثيق Documentation، على النحو التالي (محمد، 2015):

تصنيف المعلومات: وهي عملية أساسية لدى بناء أي نظام أو في بيئة أي نشاط يتعلق بالمعلومات، وتختلف التصنيفات حسب المنشأة مدار البحث، فمثلاً قد تصنف المعلومات إلى: معلومات متاحة، موثوقة، سرية، سرية للغاية، أو قد تكون معلومات متاح الوصول إليها، وأخرى محظور التوصل إليها، وهكذا.

التوثيق: تتطلب عمليات المعلومات أساساً اتباع نظام توثيق خطي لتوثيق بناء النظام وكافة وسائل المعالجة والتبادل ومكوناتها، وبشكل رئيس فإن التوثيق لازم وضروي لنظام التعريف، والتخويل Authorization وتصنيف المعلومات، والأنظمة التطبيقية، وفي إطار الأمن، فإن التوثيق يتطلب ان تكون استراتيجية أو سياسة الأمن موثقة ومكتوبة، وأن تكون إجراءاتها ومكوناتها كاملة محل توثيق، إضافة إلى خطط التعامل مع المخاطر والحوادث والجهات المسؤولة ومسؤولياتها، وخطط التعافي وإدارة الأزمات وخطط الطوارئ المرتبطة بالنظام عند حدوث الخطر.

العلاقة بين تقديم المعلومات للآخرين وتوزيعها والأمن السيبراني :

تعتبر هذه المرحلة من المراحل وثيقة الصلة بدور الأمن السيبراني في تقديم المعلومات والتأكد من وصولها لمن يطلبها، وذلك عبر عدة مراحل على النحو التالي:

أولاً: تقنيات التحقق Authentication Technologies (الطيطي، 2010):

من أجل الحفاظ على أمن المعلومات، فيجب أن يتمكن من الوصول إليها المستفيدين القانونيين فقط، وحتى يتم ذلك فلابد من تعريف المستفيد من خلال أسم المستخدم وطريقة التحقق، وأكثر الطرق شيوعاً في تعريف المستفيد هي من خلال أسم المستفيد أو التعريف ID، وغالباً ما يتم تنفيذ هذا الإجراء على النحو التالي: الاسم الأخير Last Name، الاسم الأخير مع أول حرف من الاسم الأول، تعريف الموظف Employee ID، التعريف الكامل المميز، وتوجد ثلاثة طرق رئيسة للتحقق من هوية المستخدم وهي: كلمة المرور أو جملة المرور، البطاقة الذكية، ميزة قياسية كبصمة الأصابع أو بصمة قزحية العين.

ثانياً: التخويل أو الترخيص Authorization (القحطاني، 2015):

بعد أن يصبح المستفيد معروفاً، وبعد أن تمت المصادقة على هويته، تنتقل عملية التحكم بالوصول إلى الخطوة الثانية، وهي التأكد من أن المستفيد الذي تم التعرف إليه والمصادقة على هويته لديه الصلاحيات والامتيازات التي تخوله استخدام المورد وتنفيذ العمليات التي يريدها عليه، ويُمكن تحقيق ذلك من خلال فحص قوائم التحكم بالوصول الخاصة بالمورد، لمعرفة هل لهذا المستفيد حق الاستخدام؟، وما الامتيازات والصلاحيات التي يتمتع بها؟، ومن ثم ما العمليات التي يُمكن تنفيذها على ذلك المورد؟، ويلعب التخويل دوراً رئيساً في التحكم بوصول المستخدمين إلى الموارد بشكل يضمن الاستخدام الصحيح لتلك الموارد، دونما تقييد في الصلاحيات الممنوحة وهو ما قد يخل بالعمل، ودونما إفراط في منح الصلاحيات، ينتج عنه عدم السيطرة على المورد وإساءة استخدامه، بل قد يمثل إضراراً بمصالح المنظمة أو المؤسسة.

كذلك تُستخدم وسائل السيطرة على الدخول Access Control، وذلك للحماية ضد الدخول غير المشروع إلى مصادر الأنظمة والاتصالات والمعلومات، ويشمل مفهوم الدخول غير المصرح به لأغراض خدمات الأمن الاستخدام غير المصرح به والإفشاء غير المصرح

به، والتعديل غير المصرح به، والإفشاء غير المصرح به، والاتلاف غير المصرح به، وإصدار المعلومات والأوامر غير المصرح بها، ولهذا فإن خدمات السيطرة على الدخول تُعد من الوسائل الأولية للتحقق من الدخول غير المشروع (فكري، 2015).

العلاقة بين الاحتفاظ بالمعلومات وتخزينها والأمن السيبراني :

تتعلق عمليات الاحتفاظ بالمعلومات بعمل نسخ إضافية من المواد المخزنة على إحدى وسائط التخزين، سواء داخل النظام أو خارجه، وتخضع عمليات الحفظ لقواعد يتعين أن تكون محددة سلفاً، وموثقة ومكتوبة ويجري الالتزام بها لضمان توحيد معايير الحفظ وحماية النسخ الاحتياطية، ويمثل وقت الحفظ وحماية النسخة الاحتياطية ونظام الترقيم والتبويب وآلية الاسترجاع والاستخدام، ومكان الحفظ وأمنه وتشفير النسخ التي تحتوي معطيات خاصة وسرية، مسائل رئيسة تخضع لمعايير واضحة ومحددة (محمد، 2015).

كذلك يشير الاتحاد الدولي للاتصالات (2006) إلى الأمن المادي للمعلومات باعتباره من أساسيات الأمن السيبراني، وذلك باعتبار أن المسافات الفاصلة بين مواقع محطات العمل والخوادم ومساحات وخدمات تكنولوجيا المعلومات (تكييف الهواء، لوحات الإمداد بالكهرباء، وما إلى ذلك)، تحتاج إلى حماية مادية ضد النفاذ غير المرخص به من الحوادث كالحريق، التلفيات الناتجة عن المياه، والأمن المادي هو النوع الجوهري والشائع للغاية من أنواع الرقابة على نظم تكنولوجيا المعلومات.

الدراسات السابقة:

هدفت دراسة (**الهزاني، 2018**) إلى تحديد المسؤولية الجنائية عن انتهاك قواعد الفضاء السيبراني في النظام السعودي والاماراتي، واتبعت الدراسة المنهج الوصفي التحليلي، وذلك من خلال مقارنة نصوص النظام السعودي والاماراتي في تناول انتهاك الفضاء السيبراني، وأظهرت نتائج الدراسة ما يلي: أن سبب تنامي الانتهاكات السيبرانية في معظم دول العالم يعود إلى العمل بنظرية اقليمية القانون الداخلي والقانون الدولي, من حيث عدم سريان قواعد كل منهما على الآخر، وأن معظم الدول لها تشريعاتها الخاصّة بها وفقاً لمبادئها ولا يمكن فرض قوة القانون الدولي عليها إلا بما يتعلق بأحد مسائل الفصل السابع من الشرعية الدولية، وأن الجرائم السيبرانية أشمل من الجرائم المعلوماتية حيث أن الأخيرة تعتبر جزءًا من الجرائم السيبرانية, ويعزز ذلك الأمر الملكي بإنشاء هيئة الأمن السيبراني بجانب وجود مراكز وبرامج امن المعلومات والمراكز الارشادية والتوعوية المختلفة بالمملكة العربية السعودية، كما أظهرت النتائج أن المملكة العربية السعودية ودولة الامارات من الدول المتقدمة عالمياً في توفير الخدمات الحكومية الالكترونية من خلال البوابات والمنصات الحكومية, وهذا يفرض عليهما تحدياً في مواجهة ما يسمى بالفجوة الرقمية والتي أحد نتائجها يتمثّل بتنامي الجرائم السيبرانية.

واتفقت تلك الدراسة مع الدراسة الحالية من حيث الاهتمام بتحقيق الأمن السيبراني في المملكة العربية السعودية، خاصة في ضوء توسع حكومة المملكة في تقديم الخدمات الإلكترونية، وفي حين أكدت تلك الدراسة على الشق القانوني في تحقيق الأمن السيبراني، إلا أن الدراسة الحالية قد اهتمت بدور إدارة المعلومات في هذا المجال.

وهدفت دراسة (**شلوش، 2018**) إلى التعرف على الاستراتيجيات والآليات التي يمكن تفعيلها من قبل الأنظمة الدولية لتجسيد الأمن السيبراني الدولي ومعرفة مدى علاقة القرصنة الالكترونية بإحداث تغييرات في البيئة السيبرانية الدولية، والتعرف على تأثير الهجمات السيبرانية ومنها القرصنة الالكترونية في بروز أنماط جديدة للصراع الدولي ومعرفة طبيعة هذه الهجمات السيبرانية، بالإضافة إلى التعرف على أغلب الأسلحة الالكترونية الجديدة، واتبعت الدراسة المنهج الوصفي التحليلي، واستعرضت الدراسة مفهوم الفضاء السيبراني وخصائصه، وانواع الهجمات السيبرانية وطبيعة الصراع السيبراني Cyber Conflict، وطبيعة القرصنة الإلكترونية وتهديدها للأمن العالمي، وأهمية

الأمن السيبراني لمواجهة الهجمات والجرائم السيبرانية، وتوصلت الدراسة إلى أهمية المعرفة والمعلومات ووسائل الاتصالات، فمن يملك المعرفة يتحكم في كل شيء، وأن الفضاء السيبراني واقعي، وأن الحروب السيبرانية لا مفر منها، وانها تمثل الجيل الخامس من الحروب، وان الرقمنة هي الصياغة السائدة في العصر الحالي من نقود وحكومات وسيادة سيبرانية وأمن سيبراني ودبلوماسية سيبرانية، لذا يتوجب على الدول والأفراد الحذر والحيطة عند استخدام البيانات والمعلومات في المجال الافتراضي، لتجنب الوقوع في مخاطر التصيد الشبكي والهاكرز والجماعات الإرهابية.

اتفقت تلك الدراسة مع الدراسة الحالية من حيث الاهتمام بتعرف طبيعة المخاطر السيبرانية التي تتعرض لها المنظمات أو المؤسسات الحكومية، وهو أحد محاور أداة الدراسة الحالية، واختلفت عنها من حيث الاهتمام بدور إدارة المعلومات في تحقيق الأمن السيبراني.

وهدفت دراسة (**بو سعدة، 2018**) إلى بيان دور إدارة المعلومات لأجهزة العلاقات العامة في مواجهة الأزمات التي تعترى أنشطة المؤسسات في المجتمع وإبراز أساليب وآليات استغلالها واستخدامها لتجاوز هذه الأزمات بأقل الخسائر الممكنة، وتوصلت الدراسة إلى مجموعة من النتائج أهمها: تشكل القدرة على إنتاج المعلومات خلال الأزمات والتحكم في إدارتها بصفة علمية ملاءمة قوة ناعمة تمتلكها أجهزة العلاقات العامة في المؤسسات والدول نظرا لدورها المحوري في أخذ زمام المبادرة في التعامل مع وسائل الإعلام والجمهور الداخلي والخارجي، كذلك للمعلومات دور بارز في مواجهة الأزمات المؤسساتية من خلال إتاحتها لمتخذي القرار من تحديد أسباب الأزمة والحصول على الحلول والبدائل لمواجهتها بأسلوب ناجع، تسهم إدارة المعلومات في مواجهة الأزمات من خلال بناء قواعد بيانات وتوظيفها وفق أساليب علمية دقيقة في صناعة القرار داخل المؤسسات وفى تخطيط وتنفيذ الاستراتيجيات والخطط التي من شانها مواجهة الأزمات والوقاية من حدوثها مستقبلا.

واتفقت الدراسة الحالية مع تلك الدراسة من حيث الاهتمام بدور إدارة المعلومات في مواجهة الأزمات التي تواجه المؤسسات، واختلفت عنها من حيث طبيعة تلك الأزمات، حيث شكل الأمن السيبراني محور اهتمام الدراسة الحالية.

وهدفت دراسة (**العتيبي، 2017**) إلى معرفة دور الأمن السيبراني في تعزيز الأمن الانساني، وتكونت عينة الدراسة من (400) فرد من العاملين في مجال الأمن السيبراني بشركة أرامكو السعودية فرع منطقة الرياض المجتمع، واتبعت الدراسة المنهج الوصفي التحليلي، وتم استخدام الاستبانة والمقابلة كأداتين لجمع المعلومات اللازمة للدراسة، وأظهرت نتائج الدراسة ما يلي: إن الإجراءات الفنية لحماية الفضاء السيبراني للشركة متوفرة بدرجة كبيرة، حيث يتم قفل النظام آلياً في حالة عدم استخدامه لفترة زمنية محددة، وأن الإجراءات التقنية لحماية الفضاء السيبراني الخاص بالشركة متوفرة بدرجة كبيرة، استخدام القياسات الحيوية (بصمة العين – بصمة الإصبع – بصمة الصوت) لمرور المصرح لهم، وأن سياسات الأمن السيبراني في الشركة متوفرة بدرجة كبيرة في الشركة، حيث تضمن الأنظمة آلية فعالة للإبلاغ عن أي محاولات للاختراق، وأوصت الدراسة بضرورة العمل على اتباع الوسائل العلمية والعملية لحفظ الأمن السيبراني للمؤسسات والشركات الحكومية والخاصة، وضرورة توحيد الجهود الاجتماعية والثقافية لبناء حصن منيع يحفظ الدولة وأمنها السياسي والاقتصادي والسيبراني.

واتفقت الدراسة الحالية مع تلك الدراسة من حيث عينة الدراسة، أي العاملين في مجال الأمن السيبراني، وفي حين جاء الأمن السيبراني كمتغير مستقل في تلك الدراسة، فقد جاء في الدراسة الحالية كمتغير تابع وجاءت إدارة المعلومات باعتبارها متغير مستقل في الدراسة الحالية.

أما **دراسة (الشمري، 2015)** فقد هدفت إلى تعرف أبعاد الرؤية الاستراتيجية الوطنية لحماية فضاء المملكة العربية السعودية الإلكتروني، وتكونت عينة الدراسة من جميع المختصين بأمن المعلومات الإلكترونية من المدنيين والضباط العسكريين بمدينة الرياض في مركز المعلومات الوطني، والمركز الوطني للأمن الإلكتروني، وحرس الحدود، ووزارة الكهرباء، وشركة الكهرباء، واتبعت الدراسة المنهج الوصفي التحليلي وتحليل المضمون بالإضافة إلى المنهج الاستقرائي الاستنباطي للوصول إلى أكبر قدر من مصداقية الطرائق التي سيتم استخدامها، وتوصلت

الدراسة إلى استعراض واقع حماية الفضاء الإلكتروني في المملكة العربية السعودية، و بيان مخاطر الفضاء الإلكتروني على سيادة المملكة العربية السعودية، وبيان مدى وعي المسؤولين عن أمن المعلومات بالمملكة بمخاطر الفضاء الإلكتروني، و استجلاء المعوقات التي تحد من قدرة المملكة على مواجهة مخاطر الفضاء الإلكتروني، ومن ثم تقدم الباحث بعرض رؤية استراتيجية لمواجهة مخاطر الفضاء الإلكتروني في المملكة العربية السعودية، وأوصت الدراسة بضرورة وضع رؤية استراتيجية ذات أبعاد متعددة على النحو التالي: سياسية وطنية، قانونية، عسكرية وأمنية، تعليمية وأكاديمية، اقتصادية، اقليمية ودولية، إعلامية واجتماعية) لحماية الفضاء الإلكتروني للمملكة العربية السعودية.

ويتضح من استعراض تلك الدراسة، أن الدراسة الحالية قد جاءت استجابة لتوصياتها الخاصة بوضع رؤية استراتيجية متعددة الأبعاد لتحقيق الأمن السيبراني، وعلى هذا فقد تمثل إدارة المعلومات أحد الجوانب الإدارية الخاصة بتحقيق الأمن السيبراني، وهو ما يشكل محور اهتمام الدراسة الحالية، كذلك اتفقت تلك الدراسة مع الدراسة الحالية، من حيث عينة الدراسة وهم العاملين في مجال الأمن السيبراني.

الدراسات الأجنبية

هدفت دراسة "**شوجيفار، فريكر، وجيردر**" (**Shojaifar, Fricker and Gwerder, 2018**) إلى توضيح التحديات التي تواجهها المؤسسات الصغيرة والمتوسطة الحجم فيما يتعلق بالأمن السيبراني، وأن تلك المؤسسات على الرغم من ازدياد عددها إلا أنها لا تملك نظاماً خاصاً بالأمن السيبراني، وأوضحت الدراسة أن العديد من مطوري برامج الأمن السيبراني ليست لديهم الخبرة الكافية بطبيعة عمل تلك المؤسسات وحاجتها للأمن السيبراني، لذا هدفت الدراسة إلى تعرف متطلبات الأمن السيبراني لتلك المؤسسات، وقام الباحثون بعرض إطار عمل لتوفير حاجات تلك المؤسسات من الأمن السيبراني وفق الإطار الخاص بنضج مجالات تركيز أمن المعلومات Information Security Focus Area Management (ISFAM)، والذي يشمل المواضيع التنظيمية والتقنية والدعم للأمن السيبراني، وذلك من خلال إطلاع خبراء الأمن السيبراني على طبيعة عمل تلك المؤسسات ومشاكل الهجمات السيبرانية التي تواجهها، من ثم تقديم مقترحات خبراء الأمن السيبراني لبعض الحلول المناسبة لتلك المؤسسات وفق إطار ISFAM.

وتتفق تلك الدراسة مع الدراسة الحالية فيما يتعلق بالمخاطر أو التحديات التي تواجهها المؤسسات الصغيرة فيما يتعلق بالأمن السيبراني، وهو ما يمثل أحد محاور اهتمام الدراسة الحالية، وقد اهتمت الدراسة الحالية بالإطار الخاص بنضج مجال تركيز أمن المعلومات ISFAM كإطار عمل لتحقيق الأمن السيبراني، فقد أهتمت الدراسة الحالية بدور إدارة المعلومات في هذا المجال.

وهدفت دراسة "**ميرزوا وسكوت**" (**Mierzwa & Scott, 2017**) إلى معرفة طبيعة إجراءات الأمن السيبراني في عدد من المنظمات غير الحكومية والمنظمات غير الربحية، وتم إعداد استبانة مكونة من (10) فقرات تم تطبيقها على (53) موظف من العاملين في الإدارات التقنية في تلك المنظمات، وأظهرت النتائج أن (50%) من أفراد العينة تعرضوا اثناء لمشاكل تتعلق بالبرمجيات خبيثة، أدت إلى تشفير أو قفل النظام، وأن نحو نصف تلك المنظمات لديها وحدات خاصة بالأمن السيبراني، أو موظفين مختصين بحماية شبكات المعلومات من الجرائم السيبرانية، وتتنوع وسائل الأمن السيبراني، ما بين استخدام أطر مطورة داخلياً للأمن السيبراني، أو العمل وفق معايير المعهد القومي للمعايير والتكنولوجيا National Institute for Standards and Technology (NIST) كما أوضحت استجابات أفراد العينة أن (11%) من المنظمات التي ليس لديها وحدة خاصة بالأمن السيبراني تخطط لإنشاء وحدات مماثلة خلال فترة وجيزة، وأن (53%) من موظفي تلك المنظمات تلقوا دورات تدريبية خاصة بالأمن السيبراني.

واتفقت الدراسة الحالية مع تلك الدراسة من حيث عينة الدراسة وهم العاملين في الإدارات التقنية، واتفقت معها كذلك من حيث الاهتمام بالمتطلبات الخاصة لتحقيق الأمن السيبراني، أما وجه الاختلاف فيتمثل باهتمام الدراسة الحالية بدور إدارة المعلومات في هذا المجال، أما تلك الدراسة فقد استعرضت بعض الأطر الخاصة بتحقيق الامن السيبراني.

وهدفت دراسة "**لويس وآخرون**" (**Lewis et. al., 2014**) إلى إلقاء الضوء على اختراقات الأمن السيبراني في المؤسسات الصغيرة والمتوسطة الحجم في المملكة المتحدة، حيث تمثل تلك الاختراقات نقطة ضعف رئيسة في شبكات سلاسل الإمداد التي تشارك فيها تلك المؤسسات، وخاصة في مجال تقاسم المعلومات بين الشركات الصغيرة والمتوسطة في شبكة سلسلة التوريد، مما يؤدي إلى مستوى معين من التعرض للمخاطر، وهدفت الدراسة إلى تقييم الآثار المترتبة على اعتماد مقاييس مختارة للأمن السيبراني لتقاسم المعلومات في اتحادات سلسلة التوريد الخاصة بالمؤسسات الصغيرة والمتوسطة. وبالتالي تم اختيار مجموعة من المقاييس شائعة الاستخدام في سيناريو الأمن السيبراني النموذجي واختبارها من مسح لـ 17 مؤسسة صغيرة ومتوسطة في المملكة المتحدة، ومن ثم تم تحليل النتائج فيما يتعلق بفائدة التنفيذ والاستعداد للمشاركة عبر سلاسل التوريد. وبالتالي ، واقترحت الدراسة تصنيفاً لمشاركة معلومات الأمن السيبراني لتحديد فئات التعرض للمخاطر بالنسبة للمشاريع الصغيرة والمتوسطة التي تتقاسم معلومات الأمن السيبراني، والتي يُمكن تطبيقها على تطوير اتفاقات تقاسم المعلومات (Information Sharing Agreements (ISAs داخل اتحادات سلسلة التوريد الخاصة بالمؤسسات الصغيرة والمتوسطة.

وتتفق تلك الدراسة مع الدراسة الحالية من حيث الاهتمام باختراقات الأمن السيبراني أو المخاطر السيبرانية، أما وجه الاختلاف فيتمثل في اهتمام تلك الدراسة بمجال تقاسم المعلومات، وهو أحد مجالات عمل أو وظائف إدارة المعلومات، في حين اهتمت الدراسة الحالية بدور إدارة المعلومات في تحقيق الأمن السيبراني.

وهدفت دراسة "**حسن**" (**Hassan, 2013**) إلى التعرف على أثر إدارة أمن المعلومات على فعالية تطبيق الإدارة الإلكترونية في المؤسسات الحكومية في قطاع غزة، واتبعت الدراسة المنهج الوصفي التحليلي، وتكونت عينة الدراسة من (144) موظف في المؤسسات الحكومية، وتم إعداد استبانة تكونت من (10) مجالات من مجالات إدارة أمن المعلومات وهي: سياسة الأمن، الأمن التنظيمي، ضبط الأصول وتصنيفها، الأفراد وأمن المعلومات، الأمن المكاني، إدارة الشبكة والحواسيب، ضبط الوصول للأنظمة، تطوير وصيانة الأنظمة، تخطيط استمرارية العمل، الامتثال للمتطلبات القانونية، وتوصلت الدراسة إلى أن مستوى فاعلية إدارة أمن المعلومات في المؤسسات الحكومية في قطاع غزة كان (65.3%)، وتتسم تلك الإدارة بالضعف الواضح في عدة مجالات منها: الأفراد وأمن المعلومات، الأمن التنظيمي، الامتثال للمتطلبات القانونية، تصنيف الأصول وضبطها، كما أظهرت النتائج أن مستوى فاعلية تطبيق الإدارة الإلكترونية في المؤسسات الحكومية العاملة في قطاع غزة كان (74.5%).

تتفق تلك الدراسة مع الدراسة الحالية من حيث عينة الدراسة، ومن حيث الاهتمام ببعض وظائف إدارة المعلومات، في حين اختلفت عنها من حيث المتغير التابع، فقد اهتمت تلك الدراسة بالإدارة الإلكترونية كمتغير تابع، في حين اهتمت الدراسة الحالية بالأمن السيبراني.

ويتضح من استعراض الدراسات السابقة: اتفاق الدراسة الحالية مع تلك الدراسات من حيث طبيعة المنهج المستخدم (المنهج الوصفي التحليلي)، واتفاقها مع بعض الدراسات من حيث عينة الدراسة، كذلك اتفاقها مع بعض الدراسات من حيث استخدام الاستبانة، كأداة لجمع بيانات الدراسة، أما وجه الاختلاف الرئيس فيتمثل في كون الدراسة الحالية تجمع بين متغيري إدارة المعلومات (متغير مستقل)، والأمن السيبراني (متغير تابع)، وهو ما لم يتحقق في أي من الدراسات السابقة – على حد اطلاع الباحث – وقد استفاد الباحث من الاطلاع على الدراسات السابقة من حيث إعداد أداة الدراسة الحالية، والاطلاع بشكل مفصل على إدارة المعلومات والأمن السيبراني.

إجراءات الدراسة

منهج الدراسة: تم استخدام المنهج الوصفي والذي يقوم على "دراسة الظاهرة كما توجد في الواقع و يهتم بوصفها وصفا دقيقا و يعبر عنها تعبيرا كيفيا و كميا " (عبيدات وآخرون ،2006).

ثانياً: مجتمع الدراسة وعينتها: تكون مجتمع الدراسة من جميع موظفي تقنية المعلومات في أمانة محافظة جدة باعتبارهم المختصين فيما يتعلق بالتقنية و الامن السيبراني، وبلغ عددهم 200 موظف، وبالنسبة لعينة الدراسات فينصح الإحصائيون في الدراسات الوصفية

باستخدام ما لا يقل عن 20% من أفراد المجتمع الصغير نسبيا (بضع مئات) و10% لمجتمع كبير (بضع آلاف) و5% لمجتمع كبير جدا (عشرات الآلف) (أبو النصر، 2017، ص168)، وعلى هذا الأساس فقد تم اختيار نحو 60 موظف من العاملين في تقنية المعلومات في أمانة محافظة جدة، أي ما يشكل 30% من حجم مجتمع الدراسة، ويوضح الجدول التالي توزيع أفراد العينة حسب المتغيرات التالية: المؤهل العلمي، عدد سنوات الخبرة، الجنس.

جدول (1) توزيع عينة الدراسة

المؤهل العلمي	العدد	النسبة المئوية	سنوات الخبرة	العدد	النسبة المئوية	الجنس	العدد	النسبة المئوية
دبلوم فأقل	12	%20	أقل من 10 سنوات	37	%62	ذكور	45	%75
بكالوريوس	27	%45	10 سنوات فأكثر	23	%38	إناث	15	%25
دراسات عليا	21	%35						
الإجمالي	60	%100	الإجمالي	60	%100	الإجمالي	60	%100

ثالثاً: أداة الدراسة

تم استخدام الاستبانة كأداة لجمع المعلومات والإجابة عن اسئلة الدراسة الحالية، وتتميز الاستبانة بتوفير الكثير من الوقت والجهد على الباحث في عملية جمع المعلومات، وتعطي الحرية الكاملة للمبحوث في اختيار الوقت والظروف المناسبة للإجابة عن فقراتها، والرجوع إلى ما يلزمه من مصادر، وتقلل من فرص التحيز سواء عند الباحث أو المبحوث، خاصة إذا تم صياغة فقراتها بأسلوب علمي موضوعي (بن شلهوب، 2015، ص 242)، وقام الباحث بتطبيق الاستبانة إلكترونياً مما أتاح له الإفادة من المزايا السابقة بالإضافة إلى سهولة وسرعة الحصول على استجابات أفراد العينة، وتطبيقها بشكل أقل تكلفة من الطريقة التقليدية الورقية، ويُضاف إلى ذلك سهولة نشرها، حيث يتم وضع رابط خاصة بالاستبانة يُمكن نشره بكل سهولة عبر مواقع الانترنت، وسهولة إجراء المعاملات الإحصائية.

وتم إعداد الاستبانة في ضوء ما ورد في الدراسات السابقة، بهدف تعرف دور إدارة المعلومات في تحقيق الأمن السيبراني في المنظمة، مع مراعاة صياغة فقرات الاستبانة بلغة علمية سليمة، وعدم التطرق إلى أكثر من موضوع في نفس الفقرة، وتجنب الفقرات الطويلة التي قد تشتت انتباه المبحوثين.

التحقق من صدق وثبات أداة الدراسة: تم التحقق من صدق وثبات أداة الدراسة على النحو التالي:

أ. **التحقق من صدق المحكمين:** تم عرض الاستبانة في صورتها الأولية على مجموعة من المحكمين المختصين في إدارة المعلومات والأمن السيبراني، وذلك بهدف استطلاع آرائهم حول دقة الصياغة اللغوية لفقرات الاستبانة، ووضوح تلك الصياغة وسلامتها علمياً، ومدى انتماء كل فقرة إلى المحور الذي أُدرجت فيه، وإجراء ما يلزم من تعديلات كإضافة ما يرونه من فقرات، أو حذف الفقرات غير المناسبة، وفي ضوء آراء السادة المحكمين، تم إجراء بعض التعديلات على الصورة الأولية للاستبانة.

ب. **التحقق من صدق الاتساق الداخلي للاستبانة:** تم حساب معامل الارتباط بين درجة كل فقرة والدرجة الكلية للمحور الذي تنتمي إليه، وجاءت النتائج على النحو التالي:

جدول (2) معاملات الارتباط بين درجة كل فقرة والدرجة الكلية للمحور الذي تنتمي إليه

المحور الأول		المحور الثاني		المحور الثالث	
رقم الفقرة	معامل الارتباط	رقم الفقرة	معامل الارتباط	رقم الفقرة	معامل الارتباط
1	0.649**	1	0.843**	1	0.776**
2	0.788**	2	0.630*	2	0.900**
3	0.786**	3	0.596*	3	0.838**
4	0.882**	4	0.799**	4	0.747**
5	0.964**	5	0.718**	5	0.570*
6	0.727**	6	0.634**	6	0.645**
7	0.822**	7	0.849**	7	0.645**
8	0.684**	8	0.839**	8	0.568*
		9	0.772**		
		10	0.839**		

** مستوى دلالة عند 0.01 * مستوى دلالة عند 0.05

ويتضح من النتائج السابقة أن جميع فقرات الاستبانة ترتبط بمعاملات ارتباط دالة مع الدرجة الكلية للمحور الذي تنتمي إليه، وجاءت معاملات الارتباط عند مستوى دلالة 0.05 و 0.01، وفيما بعد تم حساب معامل الارتباط بين درجة كل محور من محاور الاستبانة والدرجة الكلية للاستبانة، وجاءت النتائج على النحو التالي:

جدول (3) معاملات الارتباط بين درجة كل محور من محاور الاستبانة والدرجة الكلية للاستبانة

محاور الاستبانة	معامل الارتباط مع الدرجة الكلية للاستبانة
المخاطر السيبرانية في أمانة جدة	0.923**
متطلبات إدارة المعلومات اللازم تطبيقها لحماية الفضاء السيبراني في أمانة جدة	0.663**
التصور الاستراتيجي لتعزيز الأمن السيبراني من خلال إدارة المعلومات	0.851**

** مستوى دلالة عند 0.01

وتشير النتائج السابقة أن معاملات الارتباط بين درجة كل محور والدرجة الكلية للاستبانة، جميعها معاملات ارتباط دالة عند مستوى دلالة 0.01، وتؤكد النتائج السابقة صدق الاتساق الداخلي للاستبانة.

ج. **التحقق من ثبات الاستبانة:** تم حساب معامل الارتباط "الفا-كرونباخ" Cronbach's Alpha (α)، وذلك بالنسبة لكل محور من محاور الاستبانة وللاستبانة ككل، وجاءت النتائج على النحو الموضح في الجدول التالي:

جدول (4) قيم معامل الفا كرونباخ للاستبانة

محاور الاستبانة	عدد الفقرات	قيم معامل ألفا كرونباخ
المخاطر السيبرانية في أمانة جدة	8	0.886
متطلبات إدارة المعلومات اللازم تطبيقها لحماية الفضاء السيبراني في أمانة جدة	10	0.908
التصور الاستراتيجي لتعزيز الأمن السيبراني من خلال إدارة المعلومات	8	0.853
الاستبانة ككل	26	0.925

تشير النتائج السابقة إلى تمتع جميع محاور الاستبانة والاستبانة ككل بمعاملات ثبات عالية، وتؤكد تلك النتائج صلاحية الاستبانة ومناسبتها لتحقيق أهداف الدراسة الحالية.

إعداد الاستبانة في صورتها النهائية: بعد الانتهاء من الإجراءات السابقة، تم إعداد الاستبانة في صورتها النهائية وتكونت من قسمين على النحو التالي:

القسم الأول: يشمل البيانات الخاصة بأفراد العينة وهي: أسم المبحوث (اختياري)، المؤهل العلمي: تضمن ثلاثة مستويات وهي: الدبلوم فأقل، البكالوريوس، الدراسات العليا (ماجستير أو دكتوراه)، عدد سنوات الخبرة: وتحددت تلك السنوات في مستويين وهما: أقل من عشر سنوات، عشر سنوات فأكثر، الجنس: وتضمن مستويين (ذكر – أنثى)، تاريخ تطبيق الاستبانة

القسم الثاني: وشمل فقرات الاستبانة، وبلغ عددها 26 فقرة موزعة على ثلاثة محاور على النحو التالي: المخاطر السيبرانية في أمانة جدة وتكون من 8 فقرات، متطلبات إدارة المعلومات اللازم تطبيقها لحماية الفضاء السيبراني في أمانة جدة وتكون من 10 فقرات، التصور الاستراتيجي لتعزيز الأمن السيبراني من خلال إدارة المعلومات وتكون من 8 فقرات.

وتم تقدير استجابات أفراد العينة على فقرات الاستبانة وفقاً لمقياس ثلاثي متدرج على النحو التالي:

- اتفق بدرجة كبيرة: وتُقدر بثلاث درجات.
- اتفق إلى حد ما: وتُقدر بدرجتين.
- غير موافق: وتُقدر بدرجة واحدة.

الأساليب الإحصائية

تم استخدام برنامج الحزم الإحصائية للعلوم الاجتماعية SPSS، حيث تم ترميز بيانات الاستبانة ومعالجتها، حيث اتبعت الأساليب الإحصائية التالية:

1. معامل ارتباط "بيرسون" لحساب صدق الاتساق الداخلي للاستبانة.
2. معامل "الفا-كرونباخ" لحساب ثبات الاستبانة.
3. استخدام المتوسطات الحسابية والتكرارات لحساب استجابات أفراد العينة على الاستبانة، وتم استخدام الانحراف المعياري لحساب مدى تشتت تلك الاستجابات، وللحكم على درجة موافقة أفراد العينة على فقرات الاستبانة، ترتيب الفقرات من حيث الأولوية ودرجة الموافقة فقد تم تحديد معيار الحكم على قيم المتوسطات الحسابية على النحو التالي:

- معيار الحكم على قيم المتوسطات الحسابية وفق المعيار الثلاثي = $\frac{\text{الدرجة العليا}-\text{الدرجة الدنيا}}{\text{عدد فئات الاستجابة}}$

حيث أن الدرجة العليا = 3 درجات، والدرجة الدنيا = 1، وعدد فئات الاستجابة = 2، وعلى هذا الاساس، تم تقدير درجة الموافقة على النحو التالي:

- كبيرة: إذا كان المتوسط الحسابي أكبر من 2.33.
- متوسطة: إذا كان المتوسط الحسابي أكبر من 1.66 وأقل من 2.33.
- قليلة: إذا كان المتوسط الحسابي أقل من 1.66.

4. تحليل التباين الأحادي لمعرفة دلالة الفروق بين استجابات أفراد العينة حسب متغير المؤهل العلمي.
5. اختبار "ت" لمعرفة دلالة الفروق بين استجابات أفراد العينة حسب متغيري عدد سنوات الخبرة، والجنس.

نتائج الإجابة عن أسئلة الدراسة

السؤال الأول: ما المخاطر السيبرانية في أمانة جدة؟

جاءت نتائج استجابات أفراد العينة على المحور الأول الخاص بالمخاطر السيبرانية في أمانة جدة على النحو الموضح في الجدول التالي:

جدول (5) نتائج استجابات أفراد العينة على المحور الأول من محاور الاستبانة

م	المخاطر السيبرانية في أمانة جدة	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	الترتيب
1	فرص اختراق نظام المعلومات في أمانة جدة	2.52	0.54	كبيرة	4
2	ظاهرة ارسال الفيروسات الى أجهزة أمانة جدة	2.58	0.53	كبيرة	2
3	فرص التجسس الالكتروني على اعمال أمانة جدة	2.53	0.65	كبيرة	3
4	التخلص من وسائط التخزين التي لم يعد بحاجة لها	2.50	0.70	كبيرة	5
5	فرص نسخ البيانات بطريقة غير شرعية	2.45	0.67	كبيرة	6
6	احتمال منح صلاحيات لموظفين غير موثوق بهم	2.40	0.72	كبيرة	8
7	إجراءات عقابية لا تطال كل من يخالف الأنظمة و السياسات	2.42	0.65	كبيرة	7
8	عدم وضوح القوانين و الأنظمة الخاصة باستخدام المعلومات الالكترونية للموظفين	2.62	0.56	كبيرة	1
	الإجمالي	2.50	0.63	كبيرة	

ويتضح من تلك النتائج أن ترتيب المخاطر السيبرانية – حسب درجة موافقة أفراد العينة – ترتيباً تنازلياً على النحو التالي:

1. عدم وضوح القوانين والأنظمة الخاصة باستخدام المعلومات الإلكترونية للموظفين.
2. ظاهرة إرسال الفيروسات إلى أجهزة أمانة جدة.
3. فرص التجسس الإلكتروني على أعمال أمانة جدة.
4. فرص اختراق نظام المعلومات في أمانة جدة.
5. التخلص من وسائط التخزين التي لم يعد بحاجة إليها.
6. فرص نسخ البيانات بطريقة غير شرعية.
7. إجراءات عقابية لا تطال كل من يخالف الأنظمة و السياسات.
8. احتمال منح صلاحيات لموظفين غير موثوق بهم.

وتشير تلك النتائج إلى مخاطر تتعلق بالجانب الإداري في أمانة جدة وعلى رأسها عدم وضوح القوانين والأنظمة الخاصة باستخدام المعلومات الإلكترونية للموظفين، وعدم اتخاذ إجراءات عقابية بحق المخالفين، إضافة إلى منح صلاحيات لموظفين غير موثوق بهم، وجاء ترتيبها في المركز الأخير، أما معظم المخاطر فتتعلق بالهجمات أو الجرائم السيبرانية من خارج أمانة جدة، وهي: إرسال الفيروسات، التجسس الإلكتروني، واختراق نظام المعلومات في أمانة جدة، أما باقي المخاطر فقد تأتي من داخل أمانة جدة وتتعلق بالتخلص من وسائط التخزين التي لم تعد الأمانة بحاجة إليها، بالإضافة إلى نسخ البيانات بصورة غير شرعية.

وتشير تلك النتائج إلى دور إدارة المعلومات في تحقيق الأمن السيبراني، وذلك على النحو الذي أشار إليه (تعلب، 2010) و(الهواسي والبرزنجي، 2014) من دور إدارة المعلومات في حماية المعلومات والحفاظ على سريتها من خلال أنظمة وأدوات الحماية الإلكترونية، وهو ما يحقق الأمن السيبراني للمنظمة، وتتفق تلك النتائج مع ما أشارت إليه دراسة شوجيفار وآخرون (Shojaifar et. al.,2018)، ودراسة لويس وآخرون (Lewis et. al., 2014) حول التحديات التي تواجهها المؤسسات وتتعلق بالأمن السيبراني، ومع ما أشارت إليه دراسة حسن (Hassan, 2013) حول بعض نواحي الضعف التي تتعلق بأمن المعلومات في المنظمة.

السؤال الثاني: متطلبات إدارة المعلومات اللازم تطبيقها لحماية الفضاء السيبراني في أمانة جدة؟

جاءت نتائج استجابات أفراد العينة على المحور الثاني الخاص بمتطلبات إدارة المعلومات اللازم تطبيقها لحماية الفضاء السيبراني في أمانة جدة على النحو الموضح في الجدول التالي:

جدول (6) نتائج استجابات أفراد العينة على المحور الثاني من محاور الاستبانة

م	متطلبات إدارة المعلومات اللازم تطبيقها لحماية الفضاء السيبراني في أمانة جدة	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	الترتيب
1	التأكد من موثوقية المعلومة (بريد الكتروني، رابط)	2.83	0.38	كبيرة	1
2	وجود اليات لتناقل المعلومات المهمة والسرية	2.78	0.49	كبيرة	5
3	رصد الاختراقات لأنظمة أمانة جدة	2.81	0.39	كبيرة	3
4	استخدام برامج مكافحة الفيروسات	2.77	0.46	كبيرة	6
5	النسخ الاحتياطي للمعلومات	2.83	0.42	كبيرة	2
6	قفل النظام اليا في حالة عدم استخدامه لفترة محددة	2.72	0.52	كبيرة	8
7	تغيير كلمة المرور يتم بشكل دوري	2.75	0.51	كبيرة	7
8	إيقاف هوية المستخدم اذا بقي لفترة لم يستخدم النظام الالكتروني	2.50	0.62	كبيرة	10
9	الدورات التوعوية للعاملين حول المخاطر	2.8	0.45	كبيرة	4
10	وجود أنظمة عقابية للموظف المنتهك لسياسة أمن المعلومات	2.66	0.51	كبيرة	9
	الإجمالي	2.74	0.48	كبيرة	

ويتضح من تلك النتائج أن ترتيب متطلبات إدارة المعلومات اللازم تطبيقها لحماية الفضاء السيبراني في أمانة جدة – حسب درجة موافقة أفراد العينة – ترتيباً تنازلياً على النحو التالي:

1. التأكد من موثوقية المعلومة (بريد الكتروني، رابط)
2. النسخ الاحتياطي للمعلومات
3. رصد الاختراقات لأنظمة أمانة جدة
4. الدورات التوعوية للعاملين حول المخاطر
5. وجود اليات لتناقل المعلومات المهمة والسرية
6. استخدام برامج مكافحة الفيروسات
7. تغيير كلمة المرور يتم بشكل دوري
8. قفل النظام آلياً في حالة عدم استخدامه لفترة محددة
9. وجود أنظمة عقابية للموظف المنتهك لسياسة أمن المعلومات
10. إيقاف هوية المستخدم اذا بقي لفترة لم يستخدم النظام الالكتروني

وتوضح تلك النتائج دور إدارة المعلومات الهام في حماية الفضاء السيبراني، وذلك من خلال تحقيق معايير الأمن الأساسية CIA، والتي سبق التطرق إليها في الإطار النظري وتتعلق بموثوقية المعلومات، وتكاملها وتوافرها، كما يتعلق بدور إدارة المعلومات على النحو الذي أورده (البغدادي والعبادي، 2010) من دور لإدارة المعلومات في حماية المعلومات، وما أوردته (عصفور، 2005) من أهداف لدور المعلومات

تتمثل في الرقابة على عملية تداول البيانات وحفظها، وتتفق تلك النتائج مع ما أشارت إليه دراسة (العتيبي، 2017) من إجراءات خاصة بالأمن السيبراني كالقفل الآلي للنظام والإبلاغ عن أي اختراقات.

السؤال الثالث: التصور الاستراتيجي لتعزيز الأمن السيبراني من خلال إدارة المعلومات؟

جاءت نتائج استجابات أفراد العينة على المحور الثالث الخاص بالتصور الاستراتيجي لتعزيز الأمن السيبراني من خلال إدارة المعلومات على النحو الموضح في الجدول التالي:

جدول (7) نتائج استجابات أفراد العينة على المحور الثالث من محاور الاستبانة

م	التصور الاستراتيجي لتعزيز الأمن السيبراني من خلال إدارة المعلومات	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	الترتيب
1	استخدام مؤشرات قياس عالية	2.68	0.54	كبيرة	4
2	الاستعانة بالخبرات لتطوير وسائل الحماية	2.83	0.38	كبيرة	1
3	الشراكة مع الجهات المهتمة بالأمن السيبراني	2.77	0.50	كبيرة	2
4	تطوير نظام المراقبة (بصمة ، كاميرا)	2.60	0.53	كبيرة	6
5	توفير معامل للتجارب	2.57	0.56	كبيرة	8
6	استخدام الهكر الأخلاقي لتقييم النظام	2.60	0.62	كبيرة	7
7	تحديد صلاحيات استخدام الانترنت حسب طبيعة الوظيفة	2.62	0.64	كبيرة	5
8	زيادة الوعي من خلال الدورات و ورش العمل المتعلقة بالنواحي الأمنية	2.75	0.47	كبيرة	3
	الإجمالي	2.67	0.54	كبيرة	

ويتضح من تلك النتائج أن ترتيب الفقرات الخاصة بالتصور الاستراتيجي لتعزيز الأمن السيبراني من خلال إدارة المعلومات – حسب درجة موافقة أفراد العينة – ترتيباً تنازلياً على النحو التالي:

1. الاستعانة بالخبرات لتطوير وسائل الحماية
2. الشراكة مع الجهات المهتمة بالأمن السيبراني
3. زيادة الوعي من خلال الدورات وورش العمل المتعلقة بالنواحي الأمنية
4. استخدام مؤشرات قياس عالية
5. تحديد صلاحيات استخدام الانترنت حسب طبيعة الوظيفة
6. تطوير نظام المراقبة (بصمة ، كاميرا)
7. استخدام الهكر الأخلاقي لتقييم النظام
8. توفير معامل للتجارب

يتضح من تلك النتائج الحاجة إلى تطوير الأمن السيبراني من خلال إدارة المعلومات، وجاءت الفقرات المتعلقة بهذا التطوير في المراكز الثلاثة الأولى، حسب استجابات أفراد العينة، وذلك من خلال الإجراءات التالية: الاستعانة بالخبرات لتطوير وسائل الحماية، الشراكة مع الجهات المهتمة بالأمن السيبراني، أو رفع الكفاءة المهنية للعاملين في هذا المجال من خلال الدورات وورش العمل المتخصصة، وجاءت بعد ذلك الإجراءات الخاصة بإدارة المعلومات داخل المنظمة، وتشير تلك النتائج إلى أهمية دور إدارة المعلومات في تحقيق الأمن السيبراني، ومع ما أشارت إليه دراسة (العتيبي، 2017) من إجراءات خاصة باستخدام القياسات الحيوية ومنها (بصمة الاصبع، بصمة العين)، والحاجة إلى التدريب كما أشارت دراسة "ميرزوا وسكوت" (Mierzwa & Scott, 2017)، وأشارت تلك الدراسة إلى أهمية تطوير أساليب

الأمن السيبراني وفق معايير دولية ومنها معايير NIST وما أشارت به الدراسات السابقة لتطوير أساليب الأمن السيبراني وفق معايير محددة، ومنها دراسة شوجيفار وآخرون (Shojaifar et. al.,2018) التي أشارت إلى العمل في إطار نضج مجالات تركيز أمن المعلومات (ISFAM)، ودراسة لويس وآخرون (Lewis et. al., 2014) التي أشارت إلى اتفاقات تقاسم المعلومات (ISAs).

السؤال الرابع: هل توجد فروق ذات دلالة إحصائية بين استجابات افراد العينة بالنسبة لدور إدارة المعلومات في تحقيق الأمن السيبراني؟

للإجابة عن هذا السؤال، تم اختبار صحة فروض الدراسة على النحو التالي

أولاً: التحقق من صحة الفرض الأول، تم استخدام اختبار "ت" للتحقق من صحة الفرض الأول والذي نص على "لا توجد فروق ذات دلالة إحصائية بين استجابات افراد العينة بالنسبة لدور إدارة المعلومات في تحقيق الأمن السيبراني تُعزى لمتغير الجنس"، وجاءت النتائج على النحو الموضح في الجدول التالي:

جدول (8) دلالة الفروق بين استجابات أفراد العينة حسب متغير الجنس

دور إدارة المعلومات في تحقيق الأمن السيبراني	الجنس	العدد	المتوسط الحسابي	الانحراف المعياري	درجة الحرية	قيمة "ت"	مستوى الدلالة	الدلالة
المحور الأول	ذكر	45	2.46	0.36	58	1.56	0.123	غير دالة
	انثى	15	2.62	0.30				
المحور الثاني	ذكر	45	2.71	0.27	58	1.60	0.11	غير دالة
	انثى	15	2.83	0.13				
المحور الثالث	ذكر	45	2.63	0.36	58	1.69	0.09	غير دالة
	انثى	15	2.80	0.17				

يتضح من تلك النتائج عدم وجود فروق ذات دلالة إحصائية بين استجابات أفراد العينة تُعزى لمتغير الجنس على جميع محاور أداة الدراسة، وذلك بالنسبة لدور إدارة المعلومات في تحقيق الأمن السيبراني.

ثانياً: التحقق من صحة الفرض الثاني، تم استخدام اختبار "ت" للتحقق من صحة الفرض الثاني والذي نص على "لا توجد فروق ذات دلالة إحصائية بين استجابات افراد العينة بالنسبة لدور إدارة المعلومات في تحقيق الأمن السيبراني تُعزى لمتغير عدد سنوات الخبرة"، وجاءت النتائج على النحو الموضح في الجدول التالي:

جدول (9) دلالة الفروق بين استجابات أفراد العينة حسب متغير عدد سنوات الخبرة

دور إدارة المعلومات في تحقيق الأمن السيبراني	الخبرة	العدد	المتوسط الحسابي	الانحراف المعياري	درجة الحرية	قيمة "ت"	مستوى الدلالة	الدلالة
المحور الأول	أقل من 10 سنوات	37	2.48	0.36	58	0.615	0.541	غير دالة
	10 سنوات فأكثر	23	2.54	0.34				
المحور الثاني	أقل من 10 سنوات	37	2.75	0.26	58	0.615	0.608	غير دالة
	10 سنوات فأكثر	23	2.72	0.24				
المحور الثالث	أقل من 10 سنوات	37	2.68	0.32	58	0.158	0.875	غير دالة
	10 سنوات فأكثر	23	2.66	0.35				

يتضح من تلك النتائج عدم وجود فروق ذات دلالة إحصائية بين استجابات أفراد العينة تُعزى لمتغير عدد سنوات الخبرة على جميع محاور أداة الدراسة، وذلك بالنسبة لدور إدارة المعلومات في تحقيق الأمن السيبراني.

ثالثاً: التحقق من صحة الفرض الثالث، تم استخدام تحليل التباين الأحادي للتحقق من صحة الفرض الثالث والذي نص على "لا توجد فروق ذات دلالة إحصائية بين استجابات افراد العينة بالنسبة لدور إدارة المعلومات في تحقيق الأمن السيبراني تُعزى لمتغير المؤهل العلمي"، وجاءت النتائج على النحو الموضح في الجدول التالي:

جدول (10) دلالة الفروق بين استجابات أفراد العينة حسب متغير المؤهل العلمي

دور إدارة المعلومات في تحقيق الأمن السيبراني	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة F	مستوى الدلالة	الدلالة
المحور الأول	بين المجموعات	0.008	2	0.004	0.031	0.970	غير دالة
	داخل المجموعات	7.445	57	0.131			
	المجموع	7.453	59				
المحور الثاني	بين المجموعات	0.047	2	0.023	0.338	0.715	غير دالة
	داخل المجموعات	3.939	57	0.069			
	المجموع	3.986	59				
المحور الثالث	بين المجموعات	0.041	2	0.020	0.183	0.833	غير دالة
	داخل المجموعات	6.374	57	0.112			
	المجموع	6.415	59				

يتضح من تلك النتائج عدم وجود فروق ذات دلالة إحصائية بين استجابات أفراد العينة تُعزى لمتغير المؤهل العلمي على جميع محاور أداة الدراسة، وذلك بالنسبة لدور إدارة المعلومات في تحقيق الأمن السيبراني.

توصيات الدراسة

في ضوء النتائج السابقة، يتقدم الباحث ببعض التوصيات على النحو التالي:

1. إجراء دراسات لمعرفة مستوى تطبيق إدارة المعلومات في المؤسسات والمنظمات الحكومية، بالإضافة إلى المؤسسات الخاصة.
2. إجراء دراسات تستهدف معوقات تطبيق إدارة المعلومات في المؤسسات والمنظمات الحكومية، بالإضافة إلى المؤسسات الخاصة، وذلك في ضوء الأهمية التي تمثلها إدارة المعلومات في تحقيق الأمن السيبراني.
3. إجراء دراسات مقارنة تستهدف الاطلاع على تجارب الدول المتقدمة في تحقيق الأمن السيبراني، ودور إدارة المعلومات في هذا المجال.
4. عقد دورات تدريبية للعاملين في الإدارات التقنية بالمؤسسات المختلفة للتعريف وشرح الجانب القانوني المتعلق بالانتهاكات والاختراقات السيبرانية.
5. رفع مستوى الوعي بأهمية الأمن السيبراني لدى كافة فئات المجتمع، وذلك من خلال وسائل الإعلام، والندوات والدورات وورش العمل المختلفة، ومن خلال المناهج الدراسية، وذلك باعتبار طبيعة المخاطر التي قد تمثلها الجرائم السيبرانية على الصعيد الفردي والمجتمعي.

قائمة المراجع

أولًا: المراجع العربية:

1. أبو النصر، مدحت محمد (2017). مناهج البحث في الخدمة الاجتماعية. القاهرة: المجموعة العربية للتدريب والنشر
2. أبو شنب، ع. أ. م. (2009). إدارة وتحليل مخاطر أمن المعلومات. مؤتمر أمن المعلومات والحكومة الإلكترونية.المنظمة العربية للتنمية الإدارية – ماليزيا، كوالالمبور: المنظمة العربية للتنمية الإدارية، 1 – 18.
3. الاتحاد الدولي للاتصالات (2006). دليل الأمن السيبراني للبلدان النامية. سويسرا: مكتب تنمية الاتصالات.
4. الاتحاد الدولي للاتصالات (2010). اتجاهات الاصلاح في الاتصالات للعام 2010-2011. متاح على الرابط http://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-ar.pdf
5. برهان، محمد نور (2001). نظم المعلومات المحوسبة، القاهرة، المكتبة العصرية.
6. البغدادي، عادل هادي؛ العبادي، هاشم فوزي (2010). التعلم التنظيمي والمنظمة المتعلمة وعلاقتهما بالمفاهيم الإدارية المعاصرة. عمّان: دار الورّاق للنشر والتوزيع.
7. بن شلهوب، هيفاء بنت عبد الرحمن (2015). طرق البحث في الخدمة الاجتماعية. الرياض: مكتبة الشقري للنشر والتوزيع.
8. بوسعدة، عمر إبراهيم (2018). دور إدارة المعلومات لأجهزة العلاقات العامة في مواجهة الأزمات المؤسساتية:دراسة نظرية، مجلة بحوث العلاقات العامة الشرق الأوسط، الجمعية المصرية للعلاقات العامة، مصر، ع 18، مارس، ص ص 57-80
9. تعلب، سيد صابر (2010). نظم المعلومات الإدارية. عمّان: دار الفكر للنشر والتوزيع.
10. جبور، منى الأشقر (2012). الأمن السيبراني: التحديات ومستلزمات المواجهة. اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، جامعة الدول العربية: المركز العربي للبحوث القضائية والقانونية، بيروت، أغسطس 27 – 28.
11. حريم، حسين (2003). إدارة المنظمات من منظور كلي. عمّان: دار الحامد للنشر والتوزيع.
12. الخالد، ساري محمد (2018). اتجاهات في أمن المعلومات: أهمية تقنيات التعمية – التشفير، الرياض: مكتبة العبيكان للنشر.
13. خليفة، إيهاب (2017). القوة الإلكترونية: كيف يمكن أن تدير الدول شؤونها في عصر الإنترنت. القاهرة: دار العربي للنشر والتوزيع.
14. الربيعة، صالح بن علي (2018). الأمن السيبراني. الملتقى الأول لتقنية المعلومات "الأمن الرقمي"، وزارة التعليم – الإدارة العامة للتعليم بمحافظة جدة، أبريل: 26.
15. الردفاني، محمد قاسم أسعد (2014). تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية، المجلة العربية للدراسات الأمنية والتدريب (السعودية)، مج 30، ع 61، ديسمبر، ص ص 157-192.
16. شلوش، نورة (2018). القرصنة الإلكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول". مجلة مركز بابل للدراسات الإنسانية، المجلد 8(2)، ص 185-206.
17. الشمري، حامد بن قنيفذ (2015). رؤية استراتيجية لحماية الفضاء الإلكتروني للمملكة العربية السعودية، رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم الأمنية: كلية العلوم الاستراتيجية، قسم الدراسات الاستراتيجية.
18. الصادق، حنان بيزان (2017). دراسات ورؤى معلوماتية في إدارة المعلومات والمعرفة. القاهرة: دار حميثرا للنشر والترجمة.

19. الطيطي، خضر مصباح (2010). اساسيات أمن المعلومات والحاسوب. عمّان: دار الحامد للطباعة والنشر.
20. عبد الصادق، عادل (2017). أسلحة الفضاء الإلكتروني في ضوء القانون الدولي والإنساني، مكتبة الإسكندرية: وحدة الدراسات المستقبلية، سلسلة أوراق، العدد 23.
21. عبيدات، ذوقان وآخرون (2006). البحث العلمي مفهومه وأدواته وأساليبه. عمان:دار الفخر
22. العتيبي، عبدالرحمن بجاد (2017). دور الأمن السيبراني في تعزيز الأمن الإنساني، رسالة ماجستير غير منشورة، الرياض: جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية.
23. العسكر، فهد بن عبد الله (2013). إدارة الوثائق في عصر الاتصالات وتقنية المعلومات. القاهرة: مجموعة النيل العربية للنشر والتوزيع.
24. عصفور، أمل مصطفى (2005). نظم المعلومات الإدارية، ندوة الدعم المؤسسي والمعلومات لعمل المراكز الاستراتيجية في الحكومة، المنظمة العربية للتنمية الإدارية، شرم الشيخ، فبراير: 6-10.
25. العيسى، سمير جمال (2014). إدارة مصادر المعلومات والبيانات. عمّان: الأكاديميون للنشر والتوزيع.
26. فكري، أيمن عبد الله (2015). الجرائم المعلوماتية: دراسة مقارنة في التشريعات العربية والأجنبية. الرياض: مكتبة القانون والاقتصاد للنشر والتوزيع.
27. القحطاني، ذيب بن عايض (2015). أمن المعلومات. الرياض: مكتبة الملك عبد العزيز للعلوم والتقنية.
28. قنديلجي، عامر إبراهيم؛ السامرائي، إيمان فاضل (2002). تكنولوجيا المعلومات وتطبيقاتها. عمّان: الوراق للنشر والتوزيع.
29. محمد، جمال عبد الله (2015). نظم المعلومات الإدارية. عمّان: دار المعتز للنشر والتوزيع.
30. محمد، مالك (2013). المعلومات والأمن: رهان استراتيجي وأدوات جديدة للصراع، مؤسسة كنوز الحكمة للنشر والتوزيع، الجزائر، ع 27، ص ص 308-335.
31. مسلم، عبد الله حسن (2014). إدارة المعرفة وتكنولوجيا المعلومات. عمّان: دار المعتز للنشر والتوزيع.
32. نصيف، ع. ب. ع. ع. (2010). دور كفاية المعلومات في فاعلية اتخاذ القرارات.دراسات المعلومات، ع 9، 72.41 - .
33. نجيب، سماح (2015). الحرب العالمية الإلكترونية. القاهرة: دار التفوق.
34. نوري، حيدر شاكر؛ جمعة، محمود حسن (2013). تقييم نظام تكنولوجيا المعلومات المتكامل في المنظمات، مجلة كلية الإدارة والاقتصاد- جامعة بغداد، المجلد 19(71)، ص 166-191.
35. الهزاني، محمد بن ناصر (2018). المسؤولية الجنائية عن انتهاك قواعد الفضاء السيبراني: دراسة تأصيلية مقارنة بالقانون الإماراتي، رسالة ماجستير غير منشورة، الرياض: جامعة نايف العربية للعلوم الأمنية، كلية العدالة الجنائية.
36. الهواسي، محمود حسن؛ البرزنجي، حيدر شاكر (2014). مبادئ علم الإدارة الحديثة. بغداد: مطبعة أبن العربي.

ثانيًا: المراجع الأجنبية:

37. Canongia، C.، & Mandarino، R. (2014). Cyber security the new challenge of the information society. In Crisis Management: Concepts، Methodologies، tools and applications: 60-80. Hershey، PA: IGI Global.
38. Chen، X.، Synmann، M. & Sewdas، N. (2005). Interrelationship between document management، information management and knowledge management. South Africa journal of information management. Vol.3(7)، pp.3-17.

39. Craigen، D.، Diakun، N. & Purse، R. (2014). Defining Cyber security. Technology Innovation Management Review، Carleton University، October، pp. 13-22.
40. Goodyear، M.، Goerdel، H.، Portillo، S. & Williams، L.(2010). Cybersecurity Management in the states: the emerging role of chief information security officers، Washington: IBM center for the business of government.
41. Hassan، A. (2013). Information Security Management for strategic and effective implementation of e-management in the governmental institutions in Gaza. Unpublished master thesis، Gaza: Islamic University، Faculty of commerce.
42. Kooper، M.، Maes، R. & Lindgren، E.، (2011). On the governance of information: Introducing a new concept of governance to support the management of information. International Journal of Information Management، 31(3)، pp. 195-200.
43. Lewis، R.، Louvieris، P.، Abbot، P.، Clewley، N.، Jones، K. (2014). Cybersecurity information sharing: A framework for sustainable information security management in UK SME supply chains. Proceedings of the European conference on information systems (ECIS)، Association for information systems electronic library (AIS)، available at: http://aisel.aisnet.org/ecis2014.
44. Mierzwa، s. & Scott، J.(2017). Cybersecurity in Non-Profit and Non-Governmental Organizations. Institute for Critical Infrastructure Technology.
45. Shojaifar، A.، fricker، S.& Gwerder، M.(2018). Elicitation od SME requirements for cybersecurity solutions by studying adherence to recommendations. 24th international conference on requirements engineering: foundations for software quality. Netherlands: Utrecht University، March: 19-22.
46. Touray، A.، Salminen، A. & Marsu، A.، (2013). ICT Barriers and Critical Success Factors in Developing Countries. The Electronic Journal of Information Systems in Developing Countries، vol.56(7)، pp. 1-17.
47. Von Solms، R.، & Von Solms، S. (2015). Cyber safety education in developing countries، Systemics، cybernetics and informatics، Vol.13(2)، pp. 14-19.