المجلة العلمية لجامعة الملك فيصل
The Scientific Journal of King Faisal University
العلوم الأساسية والتطبيقية
Basic and Applied Sciences

واقع الأمن السيبراني وتحدياته في السعودية

سامي سعد السميري
قسم برامج تقنية المعلومات، معهد الإدارة العامة، جدة، المملكة العربية السعودية

The Reality of Cybersecurity and its Challenges in Saudi Arabia

Sami S. Alsemairi
Information Technology Programs Department, Institute of Public Administration, Jeddah, Saudi Arabia

LINK الرابط	RECEIVED الاستقبال	ACCEPTED القبول	PUBLISHED ONLINE النشر الإلكتروني	ASSIGNED TO AN ISSUE الإحالة لعدد
https://doi.org/10.37575/b/cmp/210075	01/11/2021	04/03/2022	04/03/2022	01/06/2022

NO. OF WORDS عدد الكلمات	NO. OF PAGES عدد الصفحات	YEAR سنة العدد	VOLUME رقم المجلد	ISSUE رقم العدد
7933	9	2022	23	1

الملخص

يشهد العالم اليوم تسارعاً في التطورات التقنية، حيث ساهمت هذه التطورات في الاستخدام المتزايد للأجهزة والمنصات والتطبيقات الإلكترونية، إذ أصبحت هذه التقنيات من العناصر المهمة في التحول الرقمي للعديد من الجهات الحكومية. لذلك صاحب هذه التطورات التقنية تطورات مماثلة في تقنيات الجرائم السيبرانية، تلك التي أضحت قضية دولية تحظى بالمزيد من الاهتمام وإحدى أولويات الأمن الوطني على صعيد العديد من دول العالم. ولأهمية هذه القضية، صدر أمر سامي كريم بإنشاء إدارة للأمن السيبراني في الجهات الحكومية في المملكة العربية السعودية وهدفها الرئيس حماية الأصول المعلوماتية والتقنية، ذلك ما يجعل الأمن السيبراني أحد أهم العناصر في تحقيق رؤية المملكة 2030. تأتي هذه الدراسة لتسليط الضوء على واقع الأمن السيبراني وتحدياته في المملكة، ولتحقيق أهداف هذه الدراسة تم تصميم استبانة إلكترونية تشمل المحاور الرئيسة التالية: إدارة الأمن السيبراني، تعامل إدارة الأمن السيبراني مع التهديدات والمخاطر السيبرانية، التقنيات أو الأساليب الأمنية المتبعة لإدارة التهديدات والمخاطرة السيبرانية، والتحديات المستقبلية (الاستراتيجية) لإدارة الأمن السيبراني. وبعد التحقق من صدق الاستبانة وثباتها، تم إرسالها إلكترونياً إلى عينة الدراسة، وقد شارك في الاستبانة (98) من موظفي تقنية المعلومات ممن يعملون في جهات حكومية مُختلفة. وقد أظهرت نتائج التحاليل الإحصائية أن مستوى واقع الأمن السيبراني في المملكة مرتفع لمواجهة التهديدات والمخاطر السيبرانية.

ABSTRACT

Recent technological developments have led to an increasingly wide use of electronic devices, platforms and applications. These technologies are now an important factor in the digital transformations taking place in many governmental agencies. In parallel with these technological advancements, new cybercrime techniques have been developed, making them a complex and highly prioritized national security issue for many countries around the world. To address this challenge, the Saudi Arabian government, through a royal decree, has urged government agencies to create internal cybersecurity departments to safeguard their information and technical assets. This makes cybersecurity a critical element of the Kingdom's 2030 Vision. This study aims to shed light on the reality of cybersecurity and its challenges in the Kingdom of Saudi Arabia. The researcher designed a questionnaire to measure several dimensions, including cybersecurity management, addressing cyber threats and risks, security techniques, and future (strategic) challenges. A sample of 98 IT employees working in different government agencies participated in this study. The results of the data analysis show that the level of cybersecurity against cyber threats and risks is high in the government agencies of Saudi Arabia.

KEYWORDS
الكلمات المفتاحية
Cybersecurity, cyberspace, cyber risks management, cyber threats and risks, cyber warfare
الأمن السيبراني، الحرب السيبرانية، الفضاء السيبراني، التهديدات والمخاطر السيبرانية، إدارة المخاطر السيبرانية

CITATION
الإحالة
Alsemairi, S.S. (2022). Waqie al'amn alsaybiranii watahadiyatuh fi alsaeudia 'The reality of cybersecurity and its challenges in Saudi Arabia'. *The Scientific Journal of King Faisal University: Basic and Applied Sciences*, **23**(1), 66 –74. DOI: 10.37575/b/cmp/210075 [in Arabic]
السميري، سامي سعد. (2022). واقع الأمن السيبراني وتحدياته في السعودية. *المجلة العلمية لجامعة الملك فيصل: العلوم الأساسية والتطبيقية*، **23**(1)، 66-74.

1. المقدمة

يشهد العالم هذه الأيام تسارعاً مستمراً يكاد لا يتوقف على صعيد تطور التقنيات الإلكترونية، والتي أصبح استخدامها ضرورة من ضروريات العصر الحالي، بل وأداة من الأدوات المهمة في التحول الرقمي، وهو ما فرض سعي أغلب الجهات الحكومية في المملكة العربية السعودية تقديم الخدمات إلكترونياً من أجل تحسين أداء الجهات الحكومية لتصبح أكثر كفاءة وفعالية (يسر، 2016). نتيجة لذلك فقد انتشر استخدام الأجهزة والمنصات والتطبيقات الإلكترونية في المملكة العربية السعودية، وزاد معها نسبة انتشار خدمات الانترنت بمعدلات عالية خلال السنوات الماضية حيث ارتفع المعدل من 82% عام 2017 إلى 93% في نهاية عام 2018 (هيئة الاتصالات وتقنية المعلومات، 2018). وإذا كان الواقع المعيش يشهد بوجود التسارع في التطور التقني واستخداماته فإنه في المقابل تطورت تقنيات التهديدات والمخاطر السيبرانية، فوفق دراسة للأمم المتحدة (UNODC, 2013)، تظهر أن نسبة مستخدمي الإنترنت الذين يقعون ضحايا المخاطر السيبرانية تتراوح بين 1 و17% وهذه النسبة تزداد في الدول النامية. والواقع أن ما أصاب كثيراً من الدول من خسائر نتيجة المخاطر السيبرانية المتطورة، وما حدث في المملكة العربية السعودية خير شاهد على ذلك، حيث حدث عام 2012 هجوم سيبراني باستخدام فيروس "شمعون"[1] على شركة أرامكو السعودية والذي كلف المملكة العربية السعودية خسائر مالية ومادية مرتفعة. ولحماية أصول تقنية المعلومات والخدمات الإلكترونية شرعت حكومة المملكة العربية السعودية لتأسيس هيئة وطنية للأمن السيبراني لجعلها المرجع الوطني لكل ما يتعلق بشؤون الأمن السيبراني، إذ فرضت "على الجهات الحكومية إنشاء إدارة مستقلة بالأمن السيبراني "أمن المعلومات" تستقل في عملها عن إدارة تقنية المعلومات، على أن يشغل رئاسة الإدارة موظف ذو كفاءة عالية في مجال الأمن السيبراني"، حتى يعمل على تحسين مستوى الأمن السيبراني للجهة الحكومية وحماية الشبكات والأنظمة والبيانات الإلكترونية. فضلاً عن التزام كل جهة حكومية بما تصدره الهيئة من سياسات وأطر ومعايير وضوابط وإرشادات (الهيئة الوطنية للأمن السيبراني، 2018). أنه وفقا ما تقدم، فإن الدراسة الراهنة تأتي لرصد الواقع المرتبط بالأمن السيبراني في الجهات الحكومية في المملكة العربية السعودية، مع التركيز بشكل خاص على إدارة الأمن السيبراني والتهديدات والمخاطر السيبرانية التي تواجهها، وذلك من خلال تطبيق المنهج الوصفي التحليلي على عينة من موظفي تقنية المعلومات في مجموعة من الجهات الحكومية داخل المملكة العربية السعودية وذلك من خلال استبانة إلكترونية صُممت لهذا الغرض.

[1] عبارة عن برنامج ضار يثبت نفسه على جهاز الضحية لحذف محتويات القرص الصلب.

Corresponding Author: Sami S. Alsemairi 00966503686862, semairis@ipa.edu.sa المؤلف المراسل: سامي سعد السميري

2. إشكالية الدراسة

تُعد الجرائم السيبرانية من أبرز التحديات الأمنية التي تواجه دول العالم بشكل عام مُشكلة تهديد وخطر سيبراني على الأصول المعلوماتية والتقنية، حيث تتصاعد معدلات الجرائم السيبرانية عاماً بعد عام مع تصاعد استخدام التقنيات الإلكترونية الحديثة مما يزيد من الخسائر المالية والتقنية، فوفق تقرير "الجرائم السيبراني لعام 2019" الصادر عن Cybersecurity Ventures[2]، أن تكلفة الجرائم السيبرانية المالية المتوقعة في العالم أكثر من 6 تريليون دولار بحلول عام 2021.

وحيث أن الجهات الحكومية في المملكة العربية السعودية -في واقعنا الحالي- تعتمد بطريقة شبه كلية على التقنيات الإلكترونية من أجل أتمتة الأعمال الإدارية، وتقديم الخدمات الإلكترونية والتكامل مع الجهات الحكومية الأخرى. لذا أصبحت هذه التقنيات (الأصول المعلوماتية والتقنية) محوراً أساسياً في تحقيق الجهات الحكومية لأهدافها، مما جعلها هدفاً للجرائم السيبرانية من قِبل أفراد مارقين أو منظمات تخريبية، مستخدمين في ذلك أدوات تقنية غير شرعية من أجل تنفيذ أهدافهم الإجرامية.

إن انتشار الجرائم السيبرانية وطبيعة تنفيذها من حيث عبورها للحدود الجغرافية للدول، يُلزم الجهات الحكومية ممثلة بإداراتها للأمن السيبراني على وضع آليات لتصدي لهذا الجرائم ومنع حدوثها، وذلك من أجل الحد من الهدر المالي والمعلوماتي، حيث ذكرت شركة IBM[3] في تقرير "تكلفة خرق البيانات لعام 2019"، أن متوسط تكلفة الاختراق في المملكة العربية السعودية بلغ 6 ملايين دولار.

لذا، تأتي هذه الدراسة لتسليط الضوء على واقع الأمن السيبراني في المملكة العربية السعودية والتحديات التي تواجهها في التصدي للجرائم السيبرانية.

3. أهداف الدراسة

تهدف هذه الدراسة في تسليط الضوء على واقع الأمن السيبراني وتحدياته في المملكة العربية السعودية. وتتضح أهداف الدراسة في النقاط التالية:

- التعرف على الدور المهم الذي تقوم به إدارة الأمن السيبراني في حماية الأصول المعلوماتية والخدمات الإلكترونية.
- تبيان التقنيات أو الأساليب الأمنية المستخدمة لإدارة التهديدات والمخاطر السيبرانية.
- الوقوف على تعامل (تفاعل) إدارة الأمن السيبراني مع التهديدات والمخاطر السيبرانية.
- رصد أبرز التحديات المستقبلية في التصدي للتهديدات والمخاطر السيبرانية.

4. أهمية الدراسة

أصبح موضوع الأمن السيبراني من بين أبرز المواضيع التي نالت اهتمام الدول في الوقت الحاضر وجزءاً أساسياً من سياساتها الوطنية، لاسيما أن الحرب السيبرانية أصبحت جزءًا لا يتجزّأ من التكتيكات الحديثة للحروب بين الدول. لذا تكمن أهمية هذه الدراسة في الكشف عن واقع الأمن السيبراني في المملكة العربية السعودية والكشف كذلك عن الدور المهم الذي تقوم به إدارات الأمن السيبراني للجهات الحكومية في حماية أصول تقنية المعلومات والخدمات الإلكترونية، الأمر الذي قد يُسهم في رفع مستوى الحماية من خطر الحرب السيبرانية وتحقيق مستوى عالي وملائم من الأمن.

تُعتبر مهمة حماية أصول تقنية المعلومات والخدمات الإلكترونية مهمة شاقة لتخللها العديد من التحديات المعقدة التي يمكن حصر أبرزها في ضرورة وجود إدارة فعالة وقادرة على التغلب على تحديات الأمن السيبراني لضمان استدامة أصول تقنية المعلومات والخدمات الإلكترونية، وهذا ما أولته المملكة العربية السعودية بالاهتمام لتنمية الجانب التقني وحماية الأصول المعلوماتية من التهديدات والمخاطر السيبرانية باعتباره أحد الركائز الاستراتيجية الأساسية لرؤية المملكة 2030، وهو ما توجه في صدور أمر ملكي رقم 6801 وتاريخ 2017/10/31، بتأسيس الهيئة الوطنية للأمن السيبراني لتكون المرجع الوطني لكل ما يتعلق بشؤون الأمن السيبراني في المملكة العربية السعودية (الهيئة الوطنية للأمن السيبراني، 2018).

5. تساؤلات الدراسة

يتحدد تساؤل الدراسة في التساؤل الرئيس التالي: ما الدور الفعلي والمستقبلي لإدارة الأمن السيبراني في الجهات الحكومية في المملكة العربية السعودية في مواجهة التهديدات والمخاطر السيبرانية؟ وللإجابة على هذا التساؤل قام الباحث بتجزئته إلى أربعة تساؤلات رئيسة هي:

- ما هو واقع إدارة الأمن السيبراني في الجهات الحكومية في المملكة العربية السعودية؟
- ما التقنيات أو الأساليب الأمنية المتبعة لإدارة التهديدات والمخاطر السيبرانية؟
- كيف تتعامل (تتفاعل) إدارة الأمن السيبراني مع التهديدات والمخاطر السيبرانية؟
- ما هي التحديات المستقبلية (الاستراتيجية) لإدارة الأمن السيبراني؟

6. الإطار النظري

ثمة مفاهيم وموضوعات متعددة تفرض نفسها في تناول موضوع الدراسة الراهنة وهي:

6.1. مفهوم الأمن السيبراني:

تطرق العديد من الباحثين والدارسين في الآونة الأخيرة إلى مفهوم الأمن السيبراني محاولين الوصول إلى صيغة موحدة، وقد حظي بمجموعة من التعريفات شأنها شأن العديد من تعاريف تقنيات المعلومات. فحسب التعريف الصادر من الهيئة الوطنية للأمن السيبراني لعام 2018 بأنه حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من عتاد وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك.

كما يعرف (Schatz *et al.,* 2017) الأمن السيبراني بأنه مجموعة الأدوات، والسياسات، والمفاهيم الأمنية، والضمانات الأمنية، والتوجيهات، ونهج إدارة المخاطر، والاجراءات، والتدريب وأفضل الممارسات، والضمان والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية والمنظمة والأصول.

ويعرفها الاتحاد الدولي للاتصالات في تقرير "اتجاهات الإصلاح في الاتصالات لعام 2010-2011" فقد تم تعريف مصطلح الأمن السيبراني بأنه "مجموعة من المهام، مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية لإدارة المخاطر، وتدريبات وأفضل الممارسات والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين".

وكذلك يعرفها (Amoroso (2006 بأنها الحد من المخاطر الضارة على البرامج وأجهزة الحاسبات والشبكات، باستخدام أدوات للكشف عن الاقتحام وايقاف الفيروسات ومنع الوصول الخبيث وفرض المصادقة وتمكين الاتصالات المشفرة.

وبناءً على ما سبق، يمكن تعريف "الأمن السيبراني" بطريقه إجرائية من منطلق هذه الدراسة بالتالي: "... بأنه العمل أو النشاط الذي يحمى الجهة الحكومية المرتبطة بالفضاء السيبراني، والحد من أضرار المخاطر والتهديدات السيبرانية باستخدام أفضل السياسات والإجراءات والتقنيات، وإعادة استمرارية العمل فوراً حال وقوع الخطر السيبراني ...".

[2] شركة إمريكية رائدة في أبحاث الأمن السيبراني على مستوى العالم.

[3] شركة استشارية وتقنية إمريكية

Alsemairi, S.S. (2022). Waqie al'amn alsaybiranii watahadiyatuh fi alsaeudia 'The reality of cybersecurity and its challenges in Saudi Arabia'. *The Scientific Journal of King Faisal University: Basic and Applied Sciences*, **23**(1), 66 –74. DOI: 10.37575/b/cmp/210075 [in Arabic]

6.2. الأمن السيبراني في المملكة:

أصبح استخدام التقنيات الإلكترونية لأهداف غير شرعية "إجرامية" خلال السنوات الماضية، يُشكل هاجس للمملكة العربية السعودية بل ولكل دول العالم، لذا أصبحت مواجهة هذه الجرائم السيبراني تحدياً على الصعيد الدولي. وأمام هذا التحدي، توكأت المملكة في تعزيز أمنها السيبراني للحد والتقليل من أثار هذه الجرائم على التالي:

- تأسيس المركز الوطني الإرشادي لأمن المعلومات عام 2006، لرفع مستوى الوعي بمخاطر أمن المعلومات ويعمل بالتعاون مع الجهات والأطراف المؤثرة على تنسيق جهود الوقاية والتصدي للتهديدات والمخاطر الالكتروني في المملكة.
- انشاء مركز التميز لأمن المعلومات عام 2008، بغرض تقديم الخدمات الاستشارية للجهات الحكومية في مجال أمن المعلومات.
- المركز الوطني للأمن الإلكتروني والذي تأسس عام 2012، للاستجابة للحوادث الإلكترونية، وحماية الفضاء الإلكتروني للمملكة ضد التهديدات الإلكترونية.
- ولادة الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز عام 2017، لكي يعمل على بناء قدرات محلية واحترافية في مجال الأمن السيبراني بناءً على أفضل الممارسات والمعايير العالمية.
- قيام الهيئة الوطنية للأمن السيبراني والذي تأسس عام 2017، لكي تقوم على إعداد الاستراتيجية الوطنية للأمن السيبراني، والإشراف على تنفيذها، وضع السياسات وآليات الحوكمة والأطر والمعايير والضوابط والإرشادات المتعلقة بالأمن السيبراني، ومتابعة الالتزام بها، وتحديثها.

وعلى الرغم من هذه الجهود الحثيثة في أطار تحقيق الأمن السيبراني فإن التقرير الإحصائي لمركز الأمن الوطني في المملكة عن التهديدات والمخاطر السيبرانية للربع الأول من عام 2018 بين أن هناك زيادة في عدد التهديدات والمخاطر بنسبة 13.5% مقارنة بالربع الأول من عام 2017. وهو ما فرض صك سياسات وإجراءات أمنية وطنية تضع ضمن أولوياتها واستراتيجياتها تحقيق الأمن السيبراني (الهيئة الوطنية للأمن السيبراني، 2018).

6.3. التهديدات والمخاطر السيبرانية:

لا توجد جهة حكومية سواءً كانت الجهة داخل المملكة العربية السعودية أو خارجها مرتبطة بالفضاء السيبراني، محصنة بشكل تام ضد التهديدات والمخاطر السيبرانية، حيث من الممكن أن تُستغل الثغرات الأمنية من قَبل المخربين للهجوم على الأصول المعلوماتية والخدمات الإلكترونية للجهة الحكومية وتدميرها. حيث يُعرف Rusi and Lehto (2017) التهديدات السيبرانية بأنها إمكانية المحاولة الضارة لتدمير أو تعطيل شبكة أو نظام حاسب آلي. ويُعرف Andress (2014) المخاطر السيبرانية بأنها مجموعة من التهديدات التي يمكن أن تؤثر سلباً على الفضاء السيبراني، مما يؤدي إلى خسائر مادية ومالية ومعنوية على حدّ سواء.

إن عملية الحماية من المخاطر السيبرانية ليست باليسيرة، وإنما هي عملية صعبة ومعقدة تتكون من ثلاث عناصر رئيسة هي: السرية، السلامة والتوافر، ذلك ما يجعل كل إجراءات الحماية من التهديدات والمخاطر السيبرانية تهدف إلى هدف واحد وهو إيصال المعلومات والبيانات والخدمات الإلكترونية إلى الأشخاص المناسبين وفي الوقت المناسب، والمحافظة على سريتها وسلامتها وهذا لا يعني شيئاً ما لم يستطع الأشخاص المخولين الوصول إليها.

وبناءً على ما سبق، يُعرف مفهوم "التهديدات والمخاطر السيبرانية" في الدراسة الراهنة بالتالي: "... بأنه نشاط سيبراني غير شرعي (إجرامي) ضد الجهة الحكومية المرتبطة بالفضاء السيبراني، حيث أن هدفها في الغالب تدمير الأصول المعلوماتية والخدمات الإلكترونية ...".

6.4. إدارة المخاطر السيبرانية:

خلال السنوات الماضية، أسست الجهات الحكومية البنية التحتية الرقمية المتصلة بشبكة الإنترنت، وازداد إعتمادها على تقديم الخدمات الإلكترونية بشكل كبير. إذ أصبحت أصول تقنية المعلومات والخدمات الإلكترونية للجهات الحكومية معرضه للمخاطر السيبرانية من أفراد مارقين أو منظمات غير شرعية. لذا ينبغي على الجهات الحكومية أن تدرك مدى المسؤولية في إدارة هذه المخاطر السيبرانية.

قبل الخوض في توضيح مفهوم "إدارة المخاطر السيبرانية"، ينبغي التطرق لتوضيح مصطلح "الإدارة"، فالإدارة عُرفت منذ القدم بالعديد من التعريفات، حيث عرفها Taylor (1911) بتحديد العمل المطلوب القيام به من قِبل العاملين، والتأكد من أدائها بأفضل السبل وأقل التكاليف. كما عرفها Fayol (1949) بأن ممارسة الإدارة تشير إلى التنبؤ بالمستقبل والتخطيط بناء عليها وإصدار الأوامر والتنسيق والمراقبة.

ومن المتداول في الأدبيات المرتبطة بالإدارة، أن هناك من يقودها في أطار تفعيل ممارساتها، ولكي أقف على المراد بها، يتوجب الإشارة إلى أن هناك جمع من التعريفات حول مفهوم "القادة" تتعدد بتعدد اغراض الدراسة وتوجهاتها المعرفية، وذلك ما يجعلها لا تأتي بتعريفه موحده.

وحيث أن موضوع الدراسة يفرض التعامل معها في سياق معرفي معين، فإن الباحث سوف يركز على بعض التعاريف في القادة. فعلى سبيل المثال عرفها Northouse (2010) بأنها "عملية يؤثر من خلالها فرد واحد على مجموعة من الأفراد بهدف تحقيق أهداف مشتركة". ويعرفها كنعان (2009) بأنها "عمل يقوم به شخص ما، ثم ينجزه آخرون حسب توجيهات هذا الشخص".

وفي الدراسة الراهنة يُشار إلى تعريف "القادة" بطريقه إجرائية بالتالي: "... أنها العمل الذي تمارسه قادة الأمن السيبراني في الجهة الحكومية لتوجيه وتحفيز أفراد الجهة من أجل تحقيق أقصى درجات الحماية الأمنية لأصول تقنية المعلومات والخدمات الإلكترونية من المخاطر السيبرانية ...".

وإذا كان المراد من مفهوم إدارة الأمن السيبراني هو تعزيز السلامة وتحقيق أقصى درجات السرية والحماية والأمان، المعهد الوطني للتقنية والمعايير (NIST) في إصداره رقم (800-39) يوصى من أجل الوفاء بما تقدم بضرورة مشاركة القادة (الإدارة العليا) في إدارة مخاطر تقنية المعلومات (NIST, 2011)، بهدف تحقيق الأمن من الجرائم السيبرانية، وإيجاد السبل الوقائية التي تمكنها من التعامل مع التهديدات السيبرانية، وتقليل خطورتها لكي تتمكن من القيام بوظائفها وأهدافها على الوجه الصحيح، كما حدد المعهد أربعة عناصر لإدارة مخاطر تقنية المعلومات وهي كالتالي: إطار المخاطر، تقييم المخاطر، الاستجابة للمخاطر، ومراقبة المخاطر.

وحرى بنا أن نسجل ها هنا، أن إتيان المعهد السالف الإشارة له بكل الاحترازات السابقة لتغليف البيانات بالسرية، فإنه يعود إلى ما تتمتع العقول المدبرة للجرائم السيبرانية ببراعة تِقنية مكافئة لنظرائهم في مجال الأمن السيبراني مما يزيد من خطورة التهديدات والمخاطر السيبرانية يوماً بعد يوم، لذا كان لزاماً على قادة الأمن السيبراني زيادة المعرفة والتعامل مع هذه التهديدات والمخاطر وفق خطوات مدروسة بأفضل الأساليب وبتطبيق أحدث تقنيات الأمن السيبراني. وفقاً لتقرير pwc لعام 2018، يُخطط 27% من قادة المنظمات للأستثمار في تقنيات الأمن السيبراني التي تستخدم الذكاء الاصطناعي والتعلم الآلي من أجل الحماية من الجرائم السيبرانية.

أنه وفق ما تقدم فإن الباحث يشير في الدراسة الراهنة إلى مفهوم "إدارة المخاطر السيبرانية" بالتالي: "... أنها مجموعة الاجراءات والأعمال الإدارية والتقنية المدروسة والمرتكزة على التخطيط السليم، والتنظيم الصحيح، والتوجيه المدروس، والقيادة الحكيمة وأخيراً الرقابة الصائبة، من قِبل القيادات التقنية، لمواجهة النشاط السيبراني غير الشرعي ...".

7. الدراسات السابقة

حظيت القضايا المرتبطة بمخاطر الأمن السيبراني بمناقشات واسعة النطاق في العديد من الدراسات السابقة خلال السنوات القليلة الماضية. ومع تزايد المخاوف بشأن هذه القضايا، بدأت العديد من الجهات الحكومية، سواءً داخل المملكة أو خارجها، في التعامل مع هذه القضايا وفق أساليب فعالة من أجل حماية أصول تقنية المعلومات والخدمات الإلكترونية. الدراسة التي أجراها (Rothrock *et al.* 2018) حددت بعض الأنظمة وأدوات المراقبة التي تُنفذها المنظمات للتعامل مع هذه القضايا،

والتي تشمل منع تسرب البيانات، وإدارة كلمات المرور، وأنظمة مراقبة المحتوى، وجدار حماية للدفاع عن حدود الشبكة الخارجية. فوفقاً لهذه الدراسة، أن هذه الأساليب توفر حلولاً تقنية لقضايا الأمن السيبراني، ولكن ليست فعالة بما فيه الكفاية للحماية الكاملة. دراسة Miranda (2018) بينت بأن التدريب الأمني للموظفين من الأساسيات في إدارة قضايا الأمن السيبراني وتحديداً إدارة المخاطر السيبرانية. كما أوصى Bauer *et al.* (2017) بأن تقوم المنظمات بتخصيص الوعي بالأمن السيبراني وبرامج التدريب على أساس مستوى الموظف ومجال المسؤولية. لذلك يُعد الوعي والتدريب الأمني جزاءاً مهماً من سياسات الأمن السيبراني ويجب أن تحدث بشكل متكرر لتحسين الوعي الأمني (Mamonov and Benbunan-Fich, 2018).

ركزت دراسة Alzubaidi (2021) على قياس المستوى الحالي للوعي بالأمن السيبراني في المملكة العربية السعودية، من حيث ممارسات الأمن السيبراني، ومستوى الوعي، والإبلاغ عن الحوادث، من خلال استبانة إلكترونية شارك في تعبئتها 1230 مشاركًا. أظهرت نتائج الاستبانة أن (31.7٪) من المشاركين استخدموا شبكة Wi-Fi عامة للوصول إلى الإنترنت، و (51٪) استخدموا معلوماتهم الشخصية لإنشاء كلمات المرور الخاصة بهم، و (32.5٪) ليس لديهم أي فكرة عن هجمات التصيد الاحتيالي، و (21.7٪) كانوا ضحية للجرائم السيبرانية بينما (29.2٪) منهم أبلغوا عن الجريمة، مما يعكس مستوى وعيهم. وتُختتم الدراسة بتقديم توصيات مبنية على تحليل النتائج لتعزيز مستوى الوعي.

ومن خلال دراسة الشمري (2015) تم استعرض واقع حماية الفضاء الإلكتروني في المملكة العربية السعودية. بالإضافة إلى توضيح بمخاطر الفضاء الإلكتروني على سيادة المملكة العربية السعودية، والوقوف على طبيعة وعي المسؤولين عن أمن المعلومات بالمملكة من مخاطر الفضاء الإلكتروني. دراسة Hu *et al.* (2012) استنتجت أن مشاركة الإدارة العليا في مبادرات أمن المعلومات لها تأثير قوي على العاملين بتوجه نحو الالتزام بالسياسات الخاصة بأمن المعلومات.

وتمحور اهتمام دراسة طاش (2015) على واقع أمن المعلومات في هيئة التحقيق والادعاء العام بالمقر الرئيس في المملكة العربية السعودية. ولخصت الدراسة نتائجها بأن إجراءات سياسات أمن المعلومات، والأمن المعلوماتي للموارد البشرية في المقر الرئيس بهيئة التحقيق والادعاء العام بالرياض مرتفعة التطبيق. أما إجراءات تقنيات الأمن المعلوماتي، وتنظيم الأمن المعلوماتي، وبيئة الأمن المعلوماتي في المقر الرئيس بالهيئة فأنها متوسطة التطبيق. وأوصت الدراسة بمجموع من التوصيات كإنشاء إدارة ذات هيكل إداري وتنظيمي لأمن المعلومات داخل الهيئة، بالإضافة إلى تدريب وتأهيل الكوادر الوطنية في إدارة أمن المعلومات. كما أوصت بتحديد المخاطر وتقييم الثغرات الأمنية التي يمكن أن تهدد أمن المعلومات داخل الهيئة. وأخيراً أوصت بتوعية العاملين بأمن المعلومات.

دراسة الشهري (2019) عرفت طبيعة الجرائم الإلكترونية وأسبابها، ووضحت المهددات والمخاطر التي تعترض الأمن السيبراني في المملكة العربية السعودية للوصول إلى رؤية استراتيجية تحد من الجرائم الإلكترونية وتعزز الأمن السيبراني. واستنتجت الدراسة بأن التقنيات الحديثة والإنترنت أدت لإنتشار الجرائم الإلكترونية، وأن أنتهاك السياسات الأمن السيبراني يمثل أهم التهديدات والمخاطر التي تواجه الفضاء السيبراني للمملكة.

دراسة Amanullah and Khan (2019) ذكرت أن الموقع الاستراتيجي للمملكة العربية السعودية في المنطقة يجعل من البنية التحتية للتقنية والمعلومات والاتصالات في القطاعين العام والخاص مهددة بإستمرار للحوادث السيبرانية، مما يؤثر على الإستقرار الإقتصادي والسياسي. كما قدمت هذه الدراسة لمحة شاملة عن رحلة المملكة في مجال الأمن السيبراني والمؤشرات التقنية المختلفة مثل الإختراقات التقنية، والقدرات السيبرانية، والحوادث السيبرانية، والاستثمارات والمبادرات الناتجة عن أبحاث الأمن السيبراني. وأخيراً، اختتمت الدراسة بإطار عمل للأمن السيبراني للمملكة، ووصت بزيادة القدرات السيبرانية الحالية من أجل إقتصاد آمن رقمياً.

وقام العويمر (2018) بالوقوف على واقع إدارة المخاطر بمركز المعلومات الوطني، وأظهرت نتائج الدراسة وجود إدارة متخصصة لإدارة المخاطر بالهيكل التنظيمي لمركز المعلومات الوطني. كما أوضح الباحث بأن المركز يقوم بتحديث البنية التحتية باستمرار وفقاً للسياسات الأمنية المتبعة فيه. بالإضافة إلى استخدام برامج أمنية من أجل استكشاف وتتبع الاختراقات وتحليلها عند تقييم المخاطر. كما أشار الباحث بإهتمام المركز بتطوير الوعي الأمني لدى الموظفين والحاقهم بالمزيد من الدورات المتخصصة في مجال أمن المعلومات.

قدم مجموعة من الباحثين (Hathaway *et al.*, 2015) إطار عمل منهجي لتقييم الجاهزية الإلكترونية لمائة وخمسة وعشرين دولة، هذه المنهجية قائمة على سبعة عناصر رئيسة هي: الاستراتيجية الوطنية، والتعامل مع الحوادث، والجريمة الإلكترونية وتطبيق القانون، ومشاركة المعلومات، والاستثمار في البحث والتطوير، والدبلوماسية والتجارة، والدفاع والتعامل مع الأزمات، تلك التي من خلالها وضعوا تصنيفاً لمدى جاهزية الدول لبعض المخاطر الإلكترونية المحددة، فضلاً عن تعيين المجالات التي يمكن تحسينها من خلال تطوير السياسات والمعايير والقوانين للحفاظ على الأمن الإلكتروني.

وألقت دراسة كلارك وكنيك (2011) الضوء على التهديدات والمخاطر الإلكترونية المحيطة بالفضاء الإلكتروني في دول الخليج، كما ناقشت نقاط ضعف الشبكات وإمكانية استهدافها لألحاق الضرر بها، وأخيراً تضع الدراسة خارطة طريق لفضاء أمن إلكترونياً. ولتأمين الفضاء السيبراني، وضعت الولايات المتحدة الإمريكية استراتيجية وطنية بهذه الخصوص عام 2003، ثم وسعت الاستراتيجية لتصبح استراتيجية دولية في عام 2011 (The White House, 2011).

كما سلطت دراسة بانقا (2019) الضوء على أهمية المخاطر السيبرانية وآثارها الإقتصادية وكيفية إدارتها، وذكرت نماذج دولية تأثرت بالهجمات السيبرانية، ثم حللت وقيّمت أوضاع دول مجلس التعاون الخليجي كدراسة حالة. وهدفت الدراسة إلى زيادة الإهتمام بالأمن السيبراني واستدراك الثغرات في التخطيط الإقتصادي لمجابهة هذه المخاطر.

أما دراسة Herhalt (2011) فبينت أن الاتصالات عبر الانترنت أصبحت قاعدة أساسية في هذا العصر، مما يسبب للحكومات مخاطر متزايدة من أن تصبح هدفاً للهجمات السيبرانية. ولمحاربة هذه الجرائم ذكرت الدراسة بأنه ينبغي على الحكومات التعاون لتطوير نموذج فعال الذي من شأنه السيطرة على هذه الجرائم. ولتخفيف من هذا الجرائم السيبرانية قدم Mylrea *et al.* (2017) إطار عمل للأمن السيبراني، هذا الإطار يزود المنظمات بمجموعة من أفضل ممارسات الأمن السيبراني، والسياسات والإجراءات من أجل تحسين وضع الأمن السيبراني.

وإذا كان الجزء النظري للأدبيات المرتبطة بموضوع الدراسة الراهنة يكشف عن مدى تباين موضوعاتها وأهدافها ونتائجها، لذلك يسلط الباحث الضوء في هذه الدراسة على الواقع الفعلي والمستقبلي للأمن السيبراني، ناهيك عن تصديها للكشف عن التحديات التي تواجهه الجهات الحكومية في المملكة العربية السعودية.

8. منهج الدراسة

في ضوء طبيعة الدراسة الراهنة، فإن الباحث يعمد إلى استخدام المنهج الوصفي، حيث يُعتبر هذا المنهج من أكثر مناهج البحث ملاءمة لهذه الدراسة بسبب إمكانية استقصاء آراء الموظفين من مختلف الجهات الحكومية. حيث تعتمد هذه الدراسة على توظيف البيانات (الأرقام) في دراسة الواقع ووصفه بشكل دقيق. وحتى يتمكن الباحث من الحصول على البيانات، فإن الباحث قام بتصميم أداة الاستبانة التي تم توجيهها إلى عينة الدراسة من موظفي تقنية المعلومات في الجهات الحكومية من أجل التعرف على الدور الفعلي والمستقبلي لإدارة الأمن السيبراني في المملكة العربية السعودية في مواجهة التهديدات والمخاطر السيبرانية. حيث شملت الاستبانة على الأبعاد التالية:

- **البُعد الإداري:** وتضمنت العبارات الخاصة بإدارة الأمن السيبراني والبالغ عددها 10 عبارات.
- **البُعد الأمني:** وتضمنت العبارات الخاصة بالتقنيات أو الأساليب الأمنية

المتبعة لإدارة التهديدات والمخاطرة السيبرانية والبالغ عددها 10 عبارات.

- **البُعد التفاعلي:** وتشمل العبارات الخاصة بتعامل (بتفاعل) إدارة الأمن السيبراني مع التهديدات والمخاطر السيبرانية والبالغ عددها 10 عبارات.
- **البُعد الاستراتيجي:** ويحتوي على العبارات الخاصة بالتحديات المستقبلية (الاستراتيجية) لإدارة الأمن السيبراني والبالغ عددها 10 عبارات.

9. مجتمع وعينة الدراسة

يتكون مجتمع الدراسة من جميع إدارات تقنية المعلومات في الجهات الحكومية في المملكة العربية السعودية، ونظراً لأن مجتمع الدراسة موزعين على جميع مناطق المملكة العربية السعودية، لذا تم الاعتماد على أسلوب المعاينة العشوائية البسيطة ليتسنى الحصول على العينة الأكثر تمثيلاً لهذا المجتمع، حيث قام الباحث بتوزيع استمارة الدراسة إلكترونياً على مجموعة من موظفي تقنية المعلومات ممن يعملون في جهات حكومية مُختلفة موزعة على جميع مناطق المملكة، والذين تلقوا التدريب في بعض البرامج التدريبية التقنية في معهد الإدارة العامة[4] خلال الفترة من أكتوبر 2018 إلى يناير 2019، إذ وفد إليه نحو (120) استمارة منها (98) استمارة مكتملة تُمثل عينة الدراسة.

10. صدق وثبات أداة الدراسة

تم قياس صدق وثبات أداة الدراسة على النحو التالي:

10.1. الصدق الظاهري:

تعتبر الاستبانة الأداة الرئيسة لهذه الدراسة والتي تتكون من أربعة محاور، حيث يشمل كل محور على 10 عبارات. وللتحقق من صدق الاستبانة عُرضت بعد صياغتها الأولية على مجموعة من المحكمين في مجال البحوث وتقنية المعلومات من منسوبي معهد الإدارة العامة؛ لمعرفة مرئياتهم حيال عبارات الاستبانة ومعرفة مدى صحة عباراتها لغوياً. وبناءً على ملاحظاتهم تم إعادة صياغة بعض العبارات.

10.2. صدق البناء:

بعد التأكد من الصدق الظاهري للاستبانة قام الباحث بحساب معاملات الارتباط بيرسون (Pearson) لمعرفة الصدق الداخلي للاستبانة من حيث مدى اتساق درجة كل عبارة من عبارات الاستبانة مع الدرجة الكلية للبُعد التي تنتمي إليه هذه العبارة.

وحيث أننا أخضعنا عبارات أداة الدراسة للقياس، حيث تبين عن معاملات الارتباط بين درجة كل عبارة من عبارات البُعد الأول (البُعد الإداري) والدرجة الكلية للبُعد موجبة حيث تراوح بين (0.624) و(0.920) وذات دلالة إحصائية عند مستوى (0.01) وبذلك يعتبر البُعد الإداري صادق لما وضع لقياسه.

ولتبيان معامل الارتباط بين كل عبارة من عبارات أداة الدراسة وفق بُعدها الأمني الذي تنتمي إليه العبارة، تبين أن معاملات الارتباط موجبة حيث تراوح بين (0.650) و(0.909) وذات دلالة إحصائية عند مستوى (0.01) وبذلك يعتبر البُعد الأمني صادق لما وضع لقياسه.

وللوقوف على درجة كل عبارة من عبارات البُعد التفاعلي (البُعد الثالث) تبين أن معاملات الارتباط موجبة حيث تراوح بين (0.834) و(0.960) وذات دلالة إحصائية عند مستوى (0.01) وبذلك يعتبر البُعد التفاعلي صادق لما وضع لقياسه.

ولتوضيح معامل الارتباط بين كل عبارة من عبارات البُعد الرابع (البُعد الاستراتيجي) والدرجة الكلية للبُعد، فإنه تبين أن معاملات الارتباط موجبة حيث تراوح بين (0.867) و(0.969) وذات دلالة إحصائية عند مستوى (0.01) وبذلك يعتبر البُعد الاستراتيجي صادق لما وضع لقياسه.

ما إذا أردنا أن نقف على قيم معاملات الارتباط لأبعاد الاستبانة مع الدرجة الكلية للاستبانة فإنها تراوحت بين (0.884) و(0.969) وذات دلالة احصائية عند مستوى ($\alpha = 0.01$)، مما يعني وجود درجة مرتفعة من صدق الاستبانة.

10.3. ثبات الأداة:

يقصد بثبات الاستبانة؛ أي أنها تُعطي نفس النتيجة عند توزيعها على عينة الدراسة أكثر من مرة في فترات زمنية معينة. ولقياس ثبات أداة الدراسة تم استخراج معامل الثبات باستخدام معامل كرونباخ ألفا (Cronbach Alpha)، ليتضح بأن قيم معامل الثبات لمحاور الدراسة تتراوح بين (0.689) و(0.888)، وبلغت قيمة معامل كرونباخ ألفا للأربعة محاور (0.814)، حيث بلغت قيمة معامل كرونباخ ألفا للأربعة محاور أكبر من (0.60) وهو الحد الأدنى الموصى بها من قبل الإحصائيين (Sekaran and Bougie, 2006)، ليتضح مما سبق صدق وثبات أداة الدراسة.

11. المعالجة الإحصائية للبيانات

وفقاً للاستجابات التي تم الحصول عليها من افراد عينة الدراسة البالغ عددهم (98) فرداً، فإن قياس الاستجابات على عبارات الاستبانة، تم باستخدام مقياس ليكرت الخماسي، حيث تم حساب المدى (مدى الدرجة)، وذلك بطرح الوزن الأدنى من الوزن الأعلى للمقياس (5-1=4)، ومن ثم تقسيمه على الوزن الأعلى للمقياس (4÷5=0.8). وبعد ذلك، يُضاف ناتج القسم إلى أدنى وزن في المقياس ليصبح طول الدرجات كما هو موضح في الجدول رقم (1):

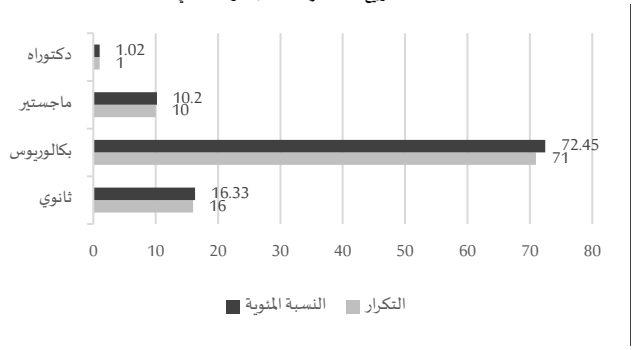
الجدول (1): المعيار المُعتمد في تفسير درجة الموافقة لأبعاد (عبارات) الدراسة

التقدير اللفظي لدرجة الموافقة	التقدير الكمي (الوزن)	الدرجة		النسبة المئوية (نسبة الموافقة)
		من	إلى	
أوافق بشدة (مرتفعة جدا)	5	4.21	5	%84.2-%100
أوافق (مرتفعة)	4	3.41	4.20	%68.2-%84
محايد (متوسطة)	3	2.61	3.40	%52.2-%68
لا أوافق (منخفضة)	2	1.81	2.60	%36.2 - %52
لا أوافق بشدة (منخفضة جدا)	1	1	1.80	%36 فاقل

وحري بنا أن نشير هنا إلى أنه يتم حساب المتوسطات الحسابية على مقياس ليكرت والانحرافات المعيارية والنسبة المئوية لاستجابات أفراد عينة الدراسة حول درجة الموافقة لكل بُعد من أبعاد الدراسة.

وحيث أن هذه الدراسة تم إجراؤها على نوعية معينة من موظفي تقنية المعلومات، فإن خصائصهم تتحدد من خلال شكل رقم (1) الذي يكشف عن أن نحو (72.45%) من عينة الدراسة يحملون درجة البكالوريوس في التخصص، وهم يمثلون أعلى الاستجابات، بينما يأتي في المرتبة الثانية من يحملون شهادة الثانوية (16.33%)، ويأتي في المرتبة الثالثة من يحملون شهادة الماجستير (10.20%)، بينما يحتل المرتبة الأخيرة من يحملون شهادة الدكتوراه (1.02%).

شكل (1): توزيع عينة الدراسة حسب المؤهل العلمي

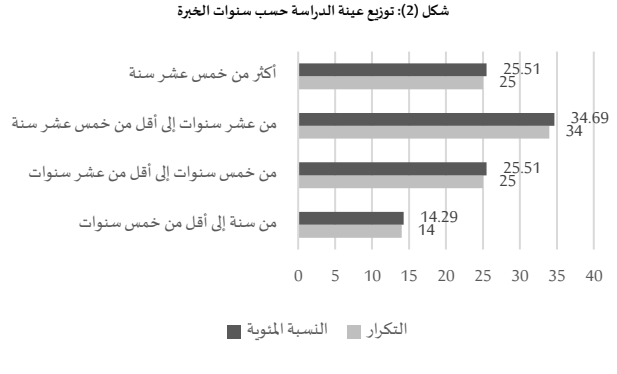


وإذا ما أردنا الوقوف على طبيعة سنوات الخبرة في مجال تقنية المعلومات، لارتباطها بعملية تطبيق قواعد ومعايير الأمن السيبراني، يتضح من شكل رقم (2) أن خبرات عينة الدراسة في أطار تقنية المعلومات قد تنوعت بتنوع سنوات الخبرة، فنجد أن من هم من عشر سنوات إلى أقل من خمس عشر سنة قد سجلوا نسبة (34.69%)، ثم يليها نسبة (25.51%) وكانت من نصيب الذي

[4] يشترط معهد الإدارة العامة للقبول على هذه البرامج أن يكون الموظف متخصص في تقنية المعلومات وممارس لهذا التخصص بما لا يقل عن سنة.

يحظون بخبرات من خمس سنوات إلى أقل من عشر سنوات وكذلك نفس النسبة من نصيب الذين يحظون بخبرات أكثر من خمس عشر سنة، بينما يأتي في المرتبة الأخيرة من سنة إلى أقل من خمس سنوات بحوالي (14.29%).

شكل (2): توزيع عينة الدراسة حسب سنوات الخبرة



12. تحليل نتائج الدراسة

إذا كنا قد أشرنا في أطار منهج الدراسة عن الأبعاد الرئيسة التي تضمنتها الاستبانة الإلكترونية، فإنه من خلال تحليلها، يمكننا الاشارة إلى ما يلي:

12.1. فيما يرتبط بالبُعد الإداري (التساؤل الأول للدراسة):

للوقوف على طبيعة البُعد الإداري في إطار تفاعلات عينة الدراسة معه فإنه يتضح من الجدول رقم (2) أن إدارة الأمن السيبراني (البُعد الإداري) جاء بدرجة موافقة مرتفعة وذلك بمتوسط حسابي مقداره (3.52) وانحراف معياري مقداره (1.36) ونسبة موافقة مقدارها (70.39%). وجاءت أعلى نسبة بمقدار (80.62%) لعبارة "المكان المخصص لأجهزة ربط الشبكة (غرفة الخوادم) مؤمن ولا يُسمح لغير المختصين بالوصول إليه"، ويعزو الباحث ذلك إلى الإجراء الإداري الذي تتبناه إدارة الأمن السيبراني في الجهات الحكومية لحماية الأصول المعلوماتية (غرفة الخوادم) لتحقيق إحدى أهم عناصر الأمن والمذكورة سابقاً ألا وهو السرية.

بينما جاءت أقل نسبة بمقدار (65.15%) لعبارة "تُوجد لجنة إشرافية متخصصة بالجهة الحكومية لمتابعة كل ما يتعلق بالأمن السيبراني"، ويعزو الباحث ذلك إلى حداثة تطبيق الأمن السيبراني في الجهات الحكومية.

جدول (2): درجة الموافقة للبُعد الإداري حسب استجابات عينة الدراسة

م	عبارات إدارة الامن السيبراني (البُعد الإداري)	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية (نسبة الموافقة)	درجة الموافقة	ترتيب العبارة
1	توجد لدى الجهة إدارة مستقلة للامن السيبراني	3.52	1.47	70.31	مرتفعة	5
2	يحظى القادة المعنيون بالأمن السيبراني بكفاءة عالية في الأمن السيبراني	3.47	1.34	69.48	مرتفعة	6
3	يتمتع العاملون بإدارة الأمن السيبراني بمهارات وكفاءات عالية في مجال الأمن السيبراني	3.42	1.31	68.45	مرتفعة	7
4	يتدرب العاملون بإدارة الامن السيبراني على المهارات الأساسية اللازمة لرفع مستوى الكفاءة	3.54	1.40	70.72	مرتفعة	3
5	توجد لدى إدارة الأمن السيبراني هيكل تنظيمي مُعتمد	3.33	1.48	66.60	متوسطة	9
6	توجد لدى إدارة الأمن السيبراني سياسات وإجراءات للأمن السيبراني	3.53	1.36	70.52	مرتفعة	4
7	تحدد الادوار والمسئوليات لجميع العاملين بإدارة الأمن السيبراني	3.34	1.40	66.80	متوسطة	8
8	توجد لجنة إشرافية متخصصة بالجهة الحكومية لمتابعة كل ما يتعلق بالأمن السيبراني	3.26	1.45	65.15	متوسطة	10
9	تطبق معايير الأمن السيبراني المعترف بها محليا ودوليا داخل الجهة الحكومية (على سبيل المثال: المعايير الأمنية لجدار الحماية)	3.76	1.27	75.26	مرتفعة	2
10	المكان المخصص لأجهزة ربط الشبكة (غرفة الخوادم) مؤمن ولا يُسمح لغير المختصين بالوصول إليه	4.03	1.15	80.62	مرتفعة	1
	إجمالي البُعد الإداري	3.52	1.36	70.39	مرتفعة	

12.2. فيما يتصل بالبُعد الأمني (التساؤل الثاني للدراسة):

من خلال عينة الدراسة، فإنه يتضح من الجدول رقم (3) أن التقنيات أو الأساليب الأمنية المتبعة لإدارة التهديدات والمخاطرة السيبرانية (البُعد الأمني) جاء بدرجة موافقة مرتفعة وذلك بمتوسط حسابي مقداره (3.92) وانحراف معياري مقداره (1.14) ونسبة موافقة مقدارها (78.41%). وجاءت أعلى نسبة بمقدار (85.31%) لعبارة "يتم حماية أجهزة الحاسب الآلي من خلال التحقق من هوية المستخدم (على سبيل المثال: استخدام اسم المستخدم وكلمة المرور)"، ويعزو الباحث ذلك إلى كونها احدى العناصر المهمة في أنظمة التحكم بالوصول. بينما جاءت أقل نسبة بمقدار (67.14%) لعبارة "لا يُسمح للأجهزة الشخصية الخاصة بالعاملين بالارتباط بشبكة الجهة الحكومية"، ويعزو الباحث ذلك إلى تطبيق الإدارة لضوابط الأمن السيبراني الخاصة بأمن الأجهزة الشخصية من أجل عدم تشكيل نقطة ضعف في الشبكة قد تُستغل من القراصنة بنشاط غير شرعي مسبّبة خطر سيبراني.

جدول (3): درجة الموافقة للبُعد الأمني حسب استجابات عينة الدراسة

م	عبارات التقنيات أو الأساليب الأمنية المتبعة لإدارة التهديدات والمخاطر السيبرانية (البُعد الأمني)	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية (نسبة الموافقة)	درجة الموافقة	ترتيب العبارة
1	توجد لدى الجهة الحكومية أنظمة وتطبيقات إلكترونية من مصادر مرخصة (على سبيل المثال: أنظمة مكافحة الفيروسات)	4.20	1.04	84.08	مرتفعة	2
2	يتم فحص ثغرات الشبكات والانظمة والتطبيقات الإلكترونية المصنفة ضمن المخاطر السيبرانية وتعالج فوراً إن وجدت	3.98	1.10	79.59	مرتفعة	5
3	تحدث حزم الأنظمة والتطبيقات الإلكترونية دوريا	3.92	1.09	78.37	مرتفعة	6
4	تستخدم تقنيات للبريد الإلكتروني في تحليل وتصفية رسائل البريد الإلكتروني خصوصاً الرسائل مجهولة المصدر	3.90	1.20	77.96	مرتفعة	7
5	يتم عمل نسخ احتياطيه للبيانات بشكل دوري	4.03	1.07	80.61	مرتفعة	8
6	تطبق متطلبات الأمن السيبراني لحماية صفحات الموقع الإلكتروني للجهة الحكومية (على سبيل المثال: استخدام بروتوكولات آمنة مثل بروتوكول https)	4.08	0.94	81.63	مرتفعة	3
7	توفر إدارة الأمن السيبراني الاحتياجات اللازمة لحماية الأصول المعلوماتية والتقنية من الفقد والسرقة والتخريب	3.78	1.13	75.51	مرتفعة	8
8	يتم حماية أجهزة الحاسب الآلي من خلال التحقق من هوية المستخدم (على سبيل المثال: استخدام اسم المستخدم وكلمة المرور)	4.27	1.01	85.31	مرتفعة جدا	1
9	يتم تغيير كلمات المرور للعاملين في الجهة الحكومية دورياً (على سبيل المثال: طلب تغيير كلمة المرور كل 90 أو 180 يوم)	3.69	1.30	73.88	مرتفعة	9
10	لا يسمح للأجهزة الشخصية الخاصة بالعاملين بالارتباط بشبكة الجهة الحكومية	3.36	1.47	67.14	متوسطة	10
	إجمالي البُعد الامني	3.92	1.14	78.41	مرتفعة	

12.3. بشأن البُعد التفاعلي (التساؤل الثالث للدراسة):

لتبيان مدى تعامل (تفاعل) إدارة الأمن السيبراني مع التهديدات والمخاطر السيبرانية حسب استجابات عينة الدراسة، فإنه من خلال الجدول رقم (4) (البُعد التفاعلي) جاء درجة الموافقة مرتفعة وذلك بمتوسط حسابي مقداره (3.48) وانحراف معياري مقداره (1.25) ونسبة موافقة مقدارها (69.61%). وجاءت أعلى نسبة بمقدار (73.06%) لعبارة "تستفيد إدارة الأمن السيبراني من المخاطر السيبرانية السابقة لتجنب الوقوع فيها مرة آخرى"، ويعزو الباحث ذلك إلى تعرف الإدارة على الثغرات الأمنية المسببة للخطر ومعالجتها لمنع تكرارها واعتبارها كدروس مستفادة. بينما جاءت أقل نسبة بمقدار (65.31%) لعبارة "تُنفذ إدارة الأمن السيبراني تجارب عملية تحاكي وقوع خطر سيبراني"، ويعزو الباحث ذلك إلى عدم وضع خطة استراتيجية لبعض إدارة الأمن السيبراني من أجل اكتشاف نقاط الضعف الأمنية الغير معروفة والتي قد تؤدي إلى تهديدات ومخاطر سيبرانية.

جدول (4): درجة الموافقة للبُعد التفاعلي حسب استجابات عينة الدراسة

م	عبارات تعامل إدارة الأمن السيبراني مع التهديدات والمخاطر السيبرانية (البُعد التفاعلي)	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية (نسبة الموافقة)	درجة الموافقة	ترتيب العبارة
1	تمتلك إدارة الأمن السيبراني الخبرة الكافية في إدارة التهديدات والمخاطر السيبرانية	3.54	1.28	70.82	مرتفعة	3
2	تمتلك إدارة الأمن السيبراني المهارة المناسبة في تحليل التهديدات والمخاطر السيبرانية ومعرفة سبب نشوئها	3.49	1.23	69.8	مرتفعة	4
3	تعمل إدارة الأمن السيبراني على استثمار جميع الإمكانيات المادية والبشرية لإدارة التهديدات والمخاطر السيبرانية	3.44	1.24	68.78	مرتفعة	8
4	تمتلك إدارة الأمن السيبراني القدرة على التكيف مع الخطر السيبراني المفاجئ	3.46	1.24	69.18	مرتفعة	7
5	توجد لدى إدارة الأمن السيبراني خطة لتوزيع المهام على العاملين أثناء الخطر السيبراني	3.40	1.25	67.96	متوسطة	9
6	تعتمد إدارة الأمن السيبراني على الحلول الحديثة في التعامل مع التهديدات والمخاطر السيبرانية	3.47	1.22	69.39	مرتفعة	5
7	تهتم إدارة الأمن السيبراني بالتنبؤ بالتهديدات والمخاطر السيبرانية وتضع برامج للتعامل معها	3.47	1.27	69.39	مرتفعة	6
8	تنفذ إدارة الأمن السيبراني تجارب عملية تحاكي وقوع خطر سيبراني	3.27	1.33	65.31	متوسطة	10
9	تقوم إدارة الأمن السيبراني بتوعية العاملين بالتهديدات والمخاطر السيبرانية دورياً	3.62	1.26	72.45	مرتفعة	2
10	تستفيد إدارة الأمن السيبراني من المخاطر السيبرانية السابقة لتجنب الوقوع فيها مرة أخرى	3.65	1.16	73.06	مرتفعة	1
	إجمالي البُعد التفاعلي	3.48	1.25	69.61	مرتفعة	

12.4. بخصوص البُعد الاستراتيجي (التساؤل الرابع للدراسة):

في ضوء ارتباط البُعد الاستراتيجي بالتحديات المستقبلية لإدارة الأمن السيبراني فإنه من خلال الجدول رقم (5) يتضح أن البُعد الاستراتيجي حظي

بدرجة موافقة مرتفعة وذلك بمتوسط حسابي مقداره (3.44) وانحراف معياري مقداره (1.31) ونسبة موافقة مقدارها (68.84%). وجاءت أعلى نسبة بمقدار (71.84%) لعبارة "تُوفر إدارة الأمن السيبراني الأدوات التقنية الحديثة للمساعدة في حماية شبكة الجهة الحكومية (على سبيل المثال: استخدام الجيل الحديث من جدران الحماية NGFW)"، ويعزو الباحث ذلك إلى أن الواقع الحالي يفرض على إدارة الأمن السيبراني الاهتمام بالتقنيات الأمنية الحديثة التي تزيد من حماية الأصول المعلوماتية ضد التهديدات والمخاطر السيبرانية. بينما جاءت أقل نسبة بمقدار (66.53%) لعبارة "تُصمم إدارة الأمن السيبراني خطة تدريب للعاملين في مجال الأمن السيبراني للحصول على الشهادات المهنية الاحترافية (على سبيل المثال: التحليل الجنائي في مجال الأمن السيبراني)"، ويعزو الباحث ذلك إلى عدم وجود خطة استراتيجية مستقبليه لبعض الجهات الحكومية في التطوير الاحترافي لمهارات موظفيها العاملين بالأمن السيبراني وهذا ما كان واضحاً في النسبة المئوية للعبارة الأولى من عبارات البُعد الاستراتيجي والمقدرة بالقيمة (67.35%).

جدول (5): درجة الموافقة للبُعد الاستراتيجي حسب استجابات عينة الدراسة

م	عبارات التحديات المستقبلية (الاستراتيجية) لإدارة الأمن السيبراني (البُعد الاستراتيجي)	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية (نسبة الموافقة)	درجة الموافقة	ترتيب العبارة
1	توجد خطة استراتيجية لإدارة الأمن السيبراني واضحة ومكتوبة	3.37	1.34	67.35	متوسط	8
2	تمتلك إدارة الأمن السيبراني رؤية ورسالة استراتيجية تعمل على تحقيقها	3.43	1.32	68.57	مرتفعة	6
3	تتواءم الخطط الاستراتيجية لإدارة الأمن السيبراني مع رؤية المملكة 2030م	3.52	1.37	70.41	مرتفعة	2
4	توجد بإدارة الأمن السيبراني كفاءات في التعامل مع التحديات المستقبلية	3.45	1.21	68.98	مرتفعة	5
5	تضع إدارة الأمن السيبراني بدائل استراتيجية للتعامل مع الأحداث المتغيرة والطارئة	3.50	1.27	70	مرتفعة	3
6	توفر إدارة الأمن السيبراني الأدوات التقنية الحديثة للمساعدة في حماية شبكة الجهة الحكومية (على سبيل المثال: استخدام الجيل الحديث من جدران الحماية NGFW)	3.59	1.25	71.84	مرتفعة	1
7	تصمم إدارة الأمن السيبراني خطة تدريب للعاملين في مجال الأمن السيبراني للحصول على الشهادات المهنية الاحترافية (على سبيل المثال: التحليل الجنائي في مجال الأمن السيبراني)	3.33	1.38	66.53	متوسطة	10
8	توجد مقاييس لتقييم أداء ومستوى الأمن السيبراني من أجل إجراء تحسينات في المستقبل القريب	3.35	1.35	66.94	متوسطة	9
9	توجد خطة استجابة للحوادث الأمنية	3.41	1.28	68.20	مرتفعة	7
10	تقوم إدارة الأمن السيبراني بتحديث الخطط الاستراتيجية للتعامل مع التحديات السيبرانية دورياً	3.48	1.30	69.59	مرتفعة	4
	إجمالي البُعد الاستراتيجي	3.44	1.31	68.84	مرتفعة	

الجدول (6): المتوسطات والانحرافات المعيارية لتقديرات عينة الدراسة على درجة الموافقة لأبعاد الدراسة

أبعاد الدراسة	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية (نسبة الموافقة)	درجة الموافقة	الترتيب
البُعد الإداري	3.52	1.36	70.39	مرتفعة	2
البُعد الأمني	3.92	1.14	78.41	مرتفعة	1
البُعد التفاعلي	3.48	1.25	69.61	مرتفعة	3
البُعد الاستراتيجي	3.44	1.31	68.84	مرتفعة	4
المتوسط العام	3.59	1.27	71.81	مرتفعة	

وإذا ما أردنا الوقوف على موقف عينة الدراسة وتقديراتهم للأبعاد الخاصة المتضمنة في الاستبانة الإلكترونية، فإنه من خلال الجدول رقم (6) يتضح لنا ما يلي:

أولاً: فيما يرتبط بدرجة الموافقة على كل بُعد من أبعاد الدراسة فإننا يمكن أن نستدل على ما يلي:

- بشأن البُعد الإداري لإدارة الأمن السيبراني: فإن استجابات عينة الدراسة جاءت على مجمل عبارات هذا البُعد بدرجة موافقة مرتفعة بمتوسط حسابي مقدر بالقيمة (3.52) وانحراف معياري مقدر بالقيمة (1.36) ونسبة موافقة مقدارها (70.39%)، وهذا يعني أن إدارات الأمن السيبراني في الجهات الحكومية تهتم بالجانب الإداري بدرجة مرتفعة.
- وحول البُعد الأمني لإدارة الأمن السيبراني: فإن استجابات عينة الدراسة على مجمل عبارات يكشف عن درجة موافقة مرتفعة بمتوسط حسابي مقدر بالقيمة (3.92) وانحراف معياري مقدر بالقيمة (1.14) ونسبة موافقة مقدارها (78.41%)، وهذا يعني أن إدارات الأمن السيبراني في الجهات الحكومية تهتم بالجانب الأمني بدرجة مرتفعة.
- فيما يرتبط بالبُعد التفاعلي لإدارة الأمن السيبراني في مواجهة التهديدات والمخاطر السيبرانية: فإن استجابات عينة الدراسة توضح أن درجة الموافقة مرتفعة بمتوسط حسابي مقدر بالقيمة (3.48) وانحراف معياري مقدر بالقيمة (1.25) ونسبة موافقة مقدارها (69.61%)، وهذا يعني أن إدارات الأمن السيبراني في الجهات الحكومية تهتم بالجانب التفاعلي بدرجة مرتفعة.
- أما البُعد الاستراتيجي لإدارة الأمن السيبراني: فإن استجابات عينة الدراسة تبين أن درجة الموافقة مرتفعة بمتوسط حسابي مقدر بالقيمة (3.44) وانحراف معياري مقدر بالقيمة (1.31) ونسبة موافقة مقدارها (68.84%)، وهذا يعني أن إدارات الأمن السيبراني في الجهات الحكومية تهتم بالجانب الاستراتيجي بدرجة مرتفعة.

ثانياً: فيما يرتبط بالنتائج العامة، فقد توصل الباحث إلى النتائج التالية:

- وفق استجابات عينة الدراسة إلى أن الواقع الفعلي للأمن السيبراني يتم تطبيقه في الجهات الحكومية بدرجة مرتفعة من وجهة نظر موظفي تقنية المعلومات في الجهات الحكومية في المملكة؛ وذلك بمتوسط عام مقدر بالقيمة (3.59)، وانحراف معياري مقدر بالقيمة (1.27) ونسبة موافقة مقدارها (71.81%)؛ مما يدل على إدراك إدارات الأمن السيبراني للتهديدات والمخاطر السيبرانية التي تواجه الجهات الحكومية في المملكة، إذ تراوحت المتوسطات الحسابية لأبعاد الدراسة بين (3.44) و (3.92) وجميعها بدرجة مرتفعة، وهذا ما يعكس التحسن الحاصل في وضعية المملكة العربية السعودية في الترتيب العالمي حسب مؤشر الرقم القياسي العالمي للأمن السيبراني الذي أصدره الإتحاد الدولي للإتصالات لعام 2018 (ITU, 2018) مقارنة بتقرير ذات الإتحاد لعام 2020 (ITU, 2020) حيث كشف تقرير عام 2018 عن احتلال المملكة المرتبة 13 عالمياً في مستوى التأهب لتهديدات ومخاطر الأمن السيبراني، بمؤشر قياس عالمي مقداره (0.881). أما في تقرير عام 2020، احتلت المملكة المرتبة 2 عالمياً بمؤشر قياس عالمي مقداره (0.9954) حسب التزامها بالمعايير التي يحددها مؤشر الرقم القياسي العالمي للأمن السيبراني والذي يهتم برصد خمسة محاور عند التقييم وهي التي تتمثل في المعايير التالية:
  - المعايير التشريعية.
  - المعايير التقنية.
  - المعايير التنظيمية.
  - بناء القدرات.
  - التعاون الدولي.

ذلك ما يعني إن جهود المملكة العربية السعودية في الأمن السيبراني ساهمت في ارتفاع مؤشر الرقم القياسي للأمن السيبراني لعام 2020 عن المؤشر لعام 2018، أذ تبوأت المملكة العربية السعودية مكانة متقدمة على مستوى الترتيب العالمي في أمنها السيبراني.

- تحتل الجوانب الأمنية والإدارية الأولوية لدى إدارات الأمن السيبراني بهدف تطبيق أفضل التقنيات الأمنية في التصدي للجرائم السيبرانية، بالإضافة إلى تعزيز وتحسين أداء العمل الإداري وذلك بتطبيق المعايير الدولية والإقليمية والمحلية في مجال الأمن السيبراني.
- أحتل البُعد الاستراتيجي المرتبة الأخيرة من أبعاد الدراسة.
- يصعب الوصول لفضاء سيبراني آمن بمستوى مرتفع جداً بين الجهات الحكومية، حيث تبقى مستويات الأمان متفاوتة، فأي جهة تعمل على تأمين ذاتها بشكل أكبر من التهديدات والمخاطر السيبرانية يرتفع مستوى الأمن السيبراني بشكل ملحوظ.

13. توصيات الدراسة

في ضوء تحقيق أهداف الدراسة وما نتج من تحليل لنتائج الدراسة نضع مجموعة من التوصيات كالتالي:

- تشكيل لجنة إشرافية متخصصة في مجال الأمن السيبراني بكل جهة حكومية لمتابعة تقييد إدارة الأمن السيبراني بضوابط الأمن السيبراني الصادرة من الهيئة الوطنية للأمن السيبراني.
- تحسين التعامل مع التهديدات والمخاطر السيبرانية من خلال تنفيذ تجارب عملية تحاكي وقوع خطر سيبراني، وذلك من أجل تقييم ومعرفة مدى جاهزية الأمن السيبراني في الجهة الحكومية.
- تأهيل موظفي الأمن السيبراني وتدريبهم بشكل دائم على التقنيات الحديثة في مجال الأمن السيبراني من أجل مراقبة الأصول المعلوماتية والتقنية وتحليل التهديدات والمخاطر السيبرانية والتصدي لها.
- ضرورة اهتمام إدارة الأمن السيبراني بالبُعد الاستراتيجي كأحد أبعاد الأمن السيبراني لتتواكب مع رؤية المملكة 2030، ومراقبة التقدم المحرز في تنفيذ الخطط الاستراتيجية.

نبذة عن المؤلف

سامي سعد السميري

قسم برامج تقنية المعلومات، معهد الإدارة العامة، جدة، المملكة العربية السعودية، semairis@ipa.edu.sa ،00966503686862

د. السميري حاصل على درجة الدكتوراه من جامعة ميرلاند - مقاطعة بالتيمور بالولايات المتحدة الإمريكية، سعودي، أعمل حالياً أستاذ مساعد ورئيساً لقسم برامج تقنية المعلومات بمعهد الإدارة العامة بمنطقة مكة المكرمة في المملكة العربية السعودية، أعمالي البحثية باللغتين (العربية والإنجليزية)، مؤسس 5 تقنيات لحماية الشبكات اللاسلكية الاستشعارية (CoDa, HART, CMBA, ASRA and BAMT)، قمت بنشر الأبحاث في المؤتمرات العالمية (IEEE WCNC, IEEE IWCMC, IEEE GLOBECOM, and IEEE WiMob) والمجلة العالمية (Wiley). اهتماماتي البحثية في مجال أمن الشبكات والاتصالات (الأمن السيبراني).

المراجع

الشمري، حامد قنيفذ. (2015). *رؤية إستراتيجية لحماية الفضاء الإلكتروني للمملكة العربية السعودية*. رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية.

الشهري، علي زايد. (2019). *رؤية استراتيجية للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية*. رسالة دكتوراه، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية.

العويمر، محمد حمد. (2018). *دور تقييم المخاطر في أمن المعلومات*. رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية.

كنعان، نواف سالم. (2005). *القيادة الإدارية*. عمان، الأردن: دار الثقافة والنشر والتوزيع.

الهيئة الوطنية للأمن السيبراني. (2018). *الضوابط الأساسية للأمن السيبراني*. متوفر بموقع: https://nca.gov.sa/files/ecc-ar.pdf (تاريخ الاسترجاع: 2019/01/08).

بانقا، علم الدين. (2019). *مخاطر الهجمات الالكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي*. الكويت: المعهد العربي للتخطيط.

برنامج التعاملات الإلكترونية الحكومية (يسر). (2016). *الخطة التنفيذية الثانية للتعاملات الإلكترونية الحكومية*. متوفر بموقع: https://www.yesser.gov.sa/for-government/digital-government-strategy-2012 (تاريخ الاسترجاع: 2019/01/23).

طارش، أحمد علي. (2015). *رؤية إستراتيجية لتحقيق الأمن المعلوماتي في هيئة التحقيق والادعاء العام في المملكة العربية السعودية*. رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية.

كلارك، ريتشارد وكنيك، روبرت. (2011). *حماية الفضاء الإلكتروني في دول مجلس التعاون الخليج العربية*. الإمارات العربية المتحدة: مركز الإمارات للدراسات والبحوث الاستراتيجية.

هيئة الاتصالات وتقنية المعلومات. (2018). *مؤشرات الأداء لقطاع الاتصالات وتقنية المعلومات*. متوفر بموقع: https://www.citc.gov.sa/ar/indicators/Pages/ICTInd2018.aspx (تاريخ الاسترجاع: 2019/04/27).

Alowaimer, M.H. (2018). *Dawr Taqyim Almakhatir fi 'Amn Almaelumat* 'Role of Risk Assessment in Information Security'. Master's Dissertation, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia. [in Arabic]

Alshammari, H.Q. (2015). *Ruyat 'listiratijiat Lihimayat Alfada' Al'iliktrunii Lilmamlakat Alearabiat Alsaeudia* 'A Strategic Vision to Protect the Cyberspace of the Kingdom of Saudi Arabia'. Master's Dissertation, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia. [in Arabic]

Alshehri, A.Z. (2019). *Ruyat Astiratijiat Lilhadi min Aljarayim Al'iliktruniat Litaeziz Al'amn Alsiybiranii fi Almamlakat Alearabiat Alsaeudia* 'A Strategic Vision to Minimize Cybercrimes and enhance Cybersecurity in the Kingdom of Saudi Arabia'. PhD Thesis, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia. [in Arabic]

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, **7**(1), e06016.

Amanullah, Q. and Khan M.K. (2019). *Cybersecurity Challenges of the Kingdom of Saudi Arabia: Past, Present and Future. Global Foundation for Cyber Studies and Research.* Available at: https://www.gfcyber.org/cybersecurity-challenges-of-the-ksa-past-present-and-future/ (accessed on 20/2/2020) [in English].

Amoroso, E. (2006). *Cyber Security*. New Jersey: Silicon Press.

Andress, J. (2014). *The Basics of Information Security - Understanding the Fundamentals of InfoSec in Theory and Practice*. 2nd edition. USA: Syngress.

Bannaga, A. (2019). *Makhatir Alhajamat Alalkitrunia (Alsiybiraniati) Watharuha Alaiqtisadiatu: Dirasat Halat Dual Majlis Altaeawun Alkhalijii'* The Risks of Cyber Attacks and Their Economic Impacts: The Case of the Gulf Cooperation Council Countries'. Kuwait: Arab Planning Institute. [in Arabic]

Bauer, S., Bernroider, E.W.N. and Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers and Security*, **68**(n/a), 145–59.

Clarke, R. and Knake, R. (2011). *Himayat Alfada' Al'iliktrunii fi Dual Majlis Altaeawun Alkhalij Alearabia* 'Securing the Gulf Cooperation Council in cyberspace'. The United Arab Emirates: The Emirates Center for Strategic Studies and Research [in Arabic]

Communications and Information Technology Commission. (2018). *Muashirat Al'ada' Liqitae Alaitisalat Watiqniat Almaelumat* 'Performance Indicators for Communications and Information Technology Sector'. Available at: https://www.citc.gov.sa/ar/indicators/Pages/ICTInd2018.aspx (accessed on 27/04/2019) [in Arabic].

e-Government Program (Yesser). (2016). *Alkhutat Altanfidhiat Althaaniat Liltaeamulat Al'iiliktruniat Alhukumia* 'The Second Operational Plan for E-Government Transactions'. Available at: https://www.yesser.gov.sa/for-government/digital-government-strategy-2012 (accessed on 23/01/2019) [in Arabic].

Fayol, H. (1949). *General and Industrial Management*. London, UK: Pitman.

Hathaway, M., Demchak C., Kerben, J., McArdle, J. and Spidalieri, F. (2015). *Cyber Readiness Index 2.0, A Plan for Cyber Readiness: A Baseline and an Index*. Potomac Institute for Policy Studies. Available at: https://www.potomacinstitute.org/images/CRIndex2.0.pdf (accessed on 16/01/2019).

Herhalt, J. (2011). Cyber Crime – A Growing Challenge for Governments. *KPMG Issues Monitor*, **8**(n/a), 1–24.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, **43**(4), 615–59.

International Telecommunication Union (ITU). (2018). *Global Cybersecurity Index (GCI) Report*. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (accessed on 09/03/2019) [in English].

International Telecommunication Union (ITU). (2020). *Global Cybersecurity Index (GCI) Report*. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (accessed on 29/06/2021) [in English].

Kanaan, N.S. (2005). *Alqiadat Al'iidaria* 'Administrative Leadership'. Amman, Jordan: Dar Althaqafa. [in Arabic]

Mamonov, S. and Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, **83**(n/a), 32–44.

Miranda, M.J. (2018). Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review*, **4**(2), 5–10.

Mylrea, M., Gourisetti, S.N.G. and Nicholls, A. (2017). An introduction to buildings cybersecurity framework, *IEEE Symposium Series on Computational Intelligence (SSCI)*. Honolulu, Hawaii, USA, 27/11-01-12/2017 [in English].

National Cybersecurity Authority. (2018). *Aldawabit Al'asasiat Lil'amn Alsiybiranii* 'Essential Cybersecurity Controls'. Available at: https://nca.gov.sa/files/ecc-ar.pdf (accessed on 08/01/2019) [in Arabic].

National Institute of Standards and Technology (NIST). (2011). *Managing Information Security Risk Organization, Mission, and Information System View*. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf (accessed on 13/01/2019).

Northouse, P. (2010). *Leadership: Theory and Practice*. 5th edition. Thousand Oaks, California: SAGE.

Tash, A.A. (2015). *Ruyat 'listratijiat Litahqiq Al'amn Almaelumatii fi Hayyat Tltahqiq Walaidiea' Aleami fi Almamlakat Alearabiat Alsaeudia* 'A Strategic Vision to Achieve Information Security in the Bureau of Investigation and Public Prosecution in the Kingdom of Saudi Arabia'. Master's Dissertation, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia. [in Arabic]

Taylor, F. (1911). *The Principles of Scientific Management*. New York, NY: Harper & Brothers.

The White House. (2011). *International Strategy for Cyberspace*. Washington

DC, USA. Available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed on 21/11/2018) [in English].

Rothrock R.A., Kaplan, J. and Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review,* **59**(2), 12–5.

Rusi, T. and Lehto, M. (2017). Cyber threats mega trends in cyber space, In: *ICCWS- Proceedings of 12th the International Conference on Cyber Warfare and Security*. Academic Conferences International. Dayton, United States, 02-03/03/2017 [in English].

Schatz, D., Bashroush, R. and Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, **12**(2), 53–74.

Sekaran, U. and Bougie, R. (2006). *Research Methods for Business A Skill-Building Approach.* 6th Edition. New York: Wiley.

United Nations Office on Drugs and Crime (UNODC). (2013). *Comprehensive Study on Cybercrime*. Available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed on 10/02/2019) [in English].