



وزارة التعليم العالي والبحث العلمي
جامعة كربلاء
كلية الإدارة والاقتصاد
قسم إدارة الأعمال

تأثير الأمن السيبراني على أداء المنظمة
دراسة استطلاعية لآراء عينة من العاملين في شركة ايرثلنك
بحث مقدم إلى مجلس كلية الإدارة والاقتصاد/ جامعة كربلاء
وهو جزء من متطلبات نيل درجة الدبلوم العالي في إدارة الجودة

كتب بواسطة:

رافد عباس حمود

بإشراف:

الاستاذ المساعد الدكتورة

أميمة حميد عبد الله



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

﴿يَرْفَعُ اللَّهُ الَّذِينَ آمَنُوا مِنْكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ وَاللَّهُ بِمَا

تَعْمَلُونَ خَبِيرٌ ﴿١١﴾﴾

صَدَقَ اللَّهُ الْعَظِيمُ

سورة المجادلة - آية مرقم (١١)

إقرار المُشرف

أشهد أن إعداد البحث الموسوم (تأثير الأمن السيبراني على أداء المنظمة/ دراسة استطلاعية لآراء عينة من العاملين في شركة ايرثلنك) الذي تقدم به طالب الدبلوم العالي (رافد عباس حمود) قد تم تحت إشرافي في جامعة كربلاء/ كلية الإدارة والاقتصاد/ قسم إدارة الاعمال، وهو جزء من متطلبات نيل درجة الدبلوم العالي في إدارة الجودة – علوم إدارة الاعمال.

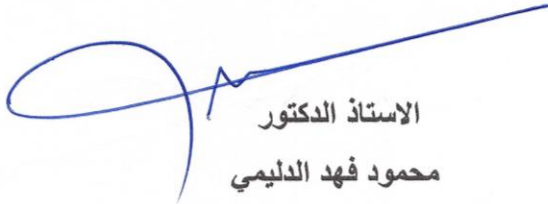

المشرف

الاستاذ المساعد الدكتورة

أميمة حميد العادلي

توصية السيد رئيس القسم:

بناء على توصية الاستاذ المشرف نرشح هذا البحث للمناقشة


الاستاذ الدكتور

محمود فهد الديمي

رئيس قسم إدارة الاعمال

2023/ 2 / 15

إقرار الخبير اللغوي

أشهد أن بحث الدبلوم العالي الموسوم (تأثير الأمن السيبراني على أداء المنظمة/ دراسة استطلاعية لأراء عينة من العاملين في شركة ايرثلنك) الذي تقدم به طالب الدبلوم العالي (رافد عباس حمود) قد راجعته من الناحية اللغوية وأصبح بأسلوب علمي سليم خالٍ من الأخطاء اللغوية ... ولأجله وقعت.



الخبير اللغوي

الاستاذ الدكتور

محمد عبد الرسول جاسم

جامعة كربلاء/ كلية التربية للعلوم الانسانية

2023/ 2 / 14

إقرار الخبير العلمي

أشهد أن بحث الدكتور العالي الموسوم (تأثير الأمن السيبراني على أداء المنظمة/ دراسة استطلاعية لآراء عينة من العاملين في شركة إيرتلينك) تم تقويمه علمياً من قبل ... ولأجله وقعت.


التوقيع:

الاسم: د. علي محمد عبد السلام

التاريخ: 2023/3/5

إقرار رئيس لجنة الدراسات العليا

بناءً على ترشيح السيد المشرف والسيد رئيس القسم وكذلك التوصية العلمية للمقومين العلمي واللغوي لبحث الدبلوم العالي في إدارة الجودة/ قسم إدارة الاعمال للطالب (رافد عباس حمود) الموسوم (تأثير الأمن السيبراني على أداء المنظمة/ دراسة استطلاعية لآراء عينة من العاملين في شركة ايرثلنك) ارشح هذا البحث للمناقشة.

رئيس لجنة الدراسات العليا

الاستاذ الدكتور

محمد حسين كاظم الجبوري

مصادقة مجلس الكلية

صادق مجلس كلية الادارة والاقتصاد/ جامعة كربلاء على توصية لجنة المناقشة

الاستاذ الدكتور

محمد حسين كاظم الجبوري

عميد كلية الإدارة والاقتصاد

أقرار لجنة المناقشة

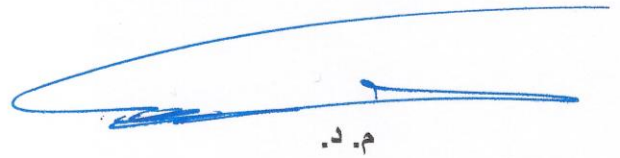
نشهد اننا رئيس واعضاء لجنة المناقشة اطلعنا على محتويات البحث الموسوم (تأثير الأمن السيبراني على أداء المنظمة/ دراسة استطلاعية لآراء عينة من العاملين في شركة ايرثلنك) الذي تقدم به طالب الدبلوم العالي (رافد عباس حمود)، وقد ناقشنا الطالب في محتوياته وفيما له علاقة به، ووجدنا أنه جدير بالقبول لنيل درجة الدبلوم العالي في علوم إدارة الاعمال بتقدير (امتياز).



عبد الحسين جاسم محمد
جامعة كربلاء/ كلية الإدارة والاقتصاد
(رئيساً)



أميمة حميد العادلي
جامعة كربلاء/ كلية الإدارة والاقتصاد
(عضوًا ومشرّفًا)



م. د. أمير غانم وادي
جامعة كربلاء/ كلية الإدارة والاقتصاد
(عضوًا)

14/3/2023

الإهداء

إلى من ارجو ان يكون علمي وعملي خالصاً لوجهه الله جل في علاه
إلى سيد الكائنات الرسول الأعظم محمد صلى الله عليه وعلى آله وسلم
إلى أئمة الهدى المطهرين تطهيراً أهل البيت عليهم افضل الصلاة وأتم التسليم
إلى بلد الحضارات وأرض السواد بلد القيم السامية العراق العظيم
إلى النبع الذي رواني حناناً وأغرقتني عطفاً ووفقتني دعاء والدتي الغالية
إلى من أفتخر بحمل اسمه وسندي في الحياة والدي العزيز
إلى ينبوع الحب والوفاء وشريكة حياتي المخلصة دوماً زوجتي الحبيبة
إلى نور العيون ونبض الفؤاد وسندي وحزام ظهري ولدي الوحيد
إلى القلوب الصافية التي تكتمل بهم سعادتي أخوتي طعم حياتي
إلى من لم يمهلها القدر لتشهد ثمرة جهدي جدتي (رحمها الله)
إلى الطيبة نفوسهم والنقية قلوبهم أصدقائي وزملاء الدراسة
إلى كل من ساعدني ومد يد العون ودعا لي بالتوفيق والنجاح الدائم
عرفاناً وتقديرًا أهدي هذا الجهد المتواضع

الباحث

شكر وتقدير

الحمد لله الذي جعل مفتاحًا لذكره وخلق الأشياء ناطقة بحمده وشكره والذي رزق البشرية العلم والمعرفة وأبعدنا عن الجهل والضلال والصلاة والسلام على نبيه محمد المشتق اسمه من اسمه المحمود وعلى آله الطيبين الطاهرين.

يسعدني وأنا أضع اللمسات الأخيرة على بحثي أن اتقدم بجزيل شكري وتقديري وامتناني للأستاذة الفاضلة الدكتورة أميمة حميد العادلي لإشرافها على هذا الجهد العلمي وتوجيهاتها السديدة له، وهي سبب نجاحي في هذا البحث لما قدمته لي من نصائح علمية ومساندتي معنويًا أدعو لها التوفيق في مسيرتها العلمية.

كما أتوجه بأسمى آيات الشكر والتقدير للسادة رئيس وأعضاء لجنة المناقشة الذين أغنوا بحثي هذا بتوجيهاتهم العلمية الدقيقة وملاحظاتهم القيمة التي ترتقي بهذا البحث نحو الأفضل.

كما أقدم اسمي آيات الشكر والتقدير إلى عمادة كلية الإدارة والاقتصاد – جامعة كربلاء عميدًا ومعاونين لجهودهم الفعالة في متابعة طلبة الدراسات العليا وتذليل الصعوبات أمامهم وإلى رئاسة واساتذة وموظفي قسم إدارة الأعمال – كلية الإدارة والاقتصاد – جامعة كربلاء الذين بذلوا ما بوسعهم في سبيل انجاح هذا البحث فلهم مني كل الاحترام والتقدير.

وشكري وتقديري إلى إدارة وموظفي شركة ايرثلنك لما بذلوه من وقت وجهد في اتمام البحث.

وفي الختام لا يسعني إلا أن اشكر كل من ساندني ودعمني ومدّ يد العون وبالخصوص السادة محكمي الاستبانة المحترمين ومن شجعني وأخص بالشكر والدتي ووالدي وزوجتي وكل أصدقائي وزملائي أمد الله تعالى بأعمارهم وسدد خطاهم وجزاهم خير الجزاء ولكل من استخدمت له مرجعًا.

وان اغفلت عن تقديم الشكر لأحد فأنتني شاكر له واسأل الله عز وجل أن يوفق الجميع لخدمة عراقنا الحبيب.

رافد عباس حمود

المستخلص

يهدف البحث إلى تسليط الضوء على متغير الأمن السيبراني وبيان تأثيره على أداء المنظمة من خلال اجراء البحث على عينة من العاملين في المقر الرئيس لشركة أيرثلنك في بغداد، تحددت مشكلة البحث بالتساؤل الرئيس والذي مضمونه (إلى أي مدى يؤثر الامن السيبراني في أداء المنظمة للشركة المبحوثة وهل تتبنى الشركة المبحوثة تطبيقات الامن السيبراني وتستثمرها في دعم اعمالها؟)، إذ تم استخدام الامن السيبراني كمتغير مستقل بثلاثة أبعاد هي (السرية، الخصوصية والتعزيز) والمتغير التابع أداء المنظمة وتحدد ببعدين (الكفاءة والفاعلية)، ومن أجل تحقيق ذلك اعتمد البحث المنهج الوصفي، وكانت العينة قصدية تضم العاملين في مجال تكنولوجيا المعلومات في الشركة المبحوثة، واستخدمت الاستبانة كأداة لجمع البيانات، إذ جرى توزيع الاستبانات على جميع افراد عينة البحث البالغ عددهم (40) موظف، وتم اعتماد مجموعة من الأساليب الاحصائية لتحليلها والتحقق من الفرضيات، ومن هذه الأساليب معامل (Cronbach Alpha) لقياس الثبات والصدق للمقياس، وتحليل الارتباط البسيط والانحدار الخطي البسيط بالاستناد إلى برنامج التحليل الاحصائي الـ (SPSS V.26)، وتم التوصل إلى مجموعة من الاستنتاجات وكان من أهمها وجود علاقة تأثير ذات دلالة معنوية للأمن السيبراني في أداء المنظمة، وان الأمن السيبراني يفسر نسبة محددة من التغيرات الحاصلة في أداء المنظمة، وكما تبين ان الشركة المبحوثة تتبنى الأمن السيبراني من خلال اهتمامها بـ (السرية، الخصوصية، والتعزيز) في أعمالها، وكما توصل الباحث إلى مجموعة من التوصيات كان من أهمها زيادة الأهتمام بالسرية سيما إدراك العاملين إلى أهمية عدم تبادل أرقام المرور السرية للأنظمة الإلكترونية العاملين عليها، وكذلك الأهتمام بصورة أكثر بالخطط الانتاجية الخاصة بعمليات المنظمة لما لها دور في تطوير الخدمات الجديدة وكونها تؤثر بصورة إيجابية على كفاءة المنظمة.

الكلمات المفتاحية: الأمن السيبراني، أداء المنظمة.

قائمة المحتويات

رقم الصفحة	الموضوع
i	الآية القرآنية
ii	الإهداء
iii	شكر وتقدير
iv	المستخلص
v	قائمة المحتويات
vi	قائمة الجداول
vii	قائمة الاشكال
vii	قائمة الملاحق
x	قائمة المختصرات
2-1	المقدمة
20-3	الفصل الأول: منهجية البحث وبعض الدراسات السابقة
3	المبحث الأول: منهجية البحث
10	المبحث الثاني: بعض الدراسات السابقة
39-21	الفصل الثاني: الجانب النظري
21	المبحث الأول: الأمن السيبراني
33	المبحث الثاني: أداء المنظمة
59-40	الفصل الثالث: الجانب العملي
40	المبحث الأول: اختبار أداة البحث
42	المبحث الثاني: التحليل الاحصائي
53	المبحث الثالث: اختبار فرضيات البحث

59-58	الفصل الرابع: الاستنتاجات والتوصيات
50	المبحث الأول: الاستنتاجات
59	المبحث الثاني: التوصيات
67-60	المصادر والمراجع
-	الملاحق

قائمة الجداول

رقم الصفحة	العنوان	رقم الجدول
7	وصف عينة البحث	1
10	الدراسات العربية السابقة الخاصة بمتغير الأمن السيبراني	2
12	الدراسات الأجنبية السابقة الخاصة بمتغير الأمن السيبراني	3
15	الدراسات العربية السابقة الخاصة بمتغير أداء المنظمة	4
17	الدراسات الأجنبية السابقة الخاصة بمتغير أداء المنظمة	5
22	تعريفات الأمن السيبراني	6
34	تعريفات أداء المنظمة	7
41	معامل الثبات Cronbach's Alpha لمتغيرات البحث	8
42	الايوساط الحسابية الموزونة ومستويات الاجابة لها	9
43	الإحصاءات الوصفية لبعء السرية	10
44	الإحصاءات الوصفية لبعء الخصوصية	11
46	الإحصاءات الوصفية لبعء التعزيز	12
48	ترتيب ابعاد الأمن السيبراني	13
49	الإحصاءات الوصفية لبعء الكفاءة	14
50	الإحصاءات الوصفية لبعء الفاعلية	15
52	ترتيب ابعاد أداء المنظمة	16
54	أختبار الفرضية الرئيسية الاولى (فرضية الارتباط)	17
55	تقدير علاقة الانحدار الخطي البسيط بين الأمن السيبراني واداء المنظمة	18

قائمة الأشكال

رقم الصفحة	العنوان	رقم الشكل
6	المخطط الفرضي للبحث	1
25	فوائد الأمتثال لمعايير الأمن السيبراني في المنظمات ..	2
26	أثار الهجوم الإلكتروني على المنظمة	3
28	أنواع الامن السيبراني	4
39	العلاقة بين الفاعلية والكفاءة	5

قائمة الملاحق

العنوان	رقم الملحق
أداة القياس	1
أسماء السادة محكمي أداة القياس	2
الاستبانة	3
قيم T الجدولية	4
قيم F الجدولية	5

قائمة المختصرات

المختصر	المعنى باللغة الانكليزية	المعنى باللغة العربية
COBIT5	Control Objectives for Information and related Technology.	هو إطار الأعمال والإدارة الشامل لحوكمة وإدارة تكنولوجيا المعلومات في المؤسسة.
NVivo	NVivo is a qualitative data analysis (QDA) computer software package produced by QSR Internationa.	عبارة عن حزمة برامج كمبيوتر لتحليل البيانات النوعية أنتجت بواسطة QSR International.
MITM	Man-in-the-middle attack	هجوم الوسيط في التشفير وأمن الحاسوب هو نوع من الاختراق حيث يتسلل المهاجم بين متحاورين في شبكة دون علم كل منهما.
SQL	Structured Query Language	لغة الاستعلام المهيكل اختصاراً SQL.
SEM	Structural Equation Modeling	نمذجة المعادلات الهيكلية هي تسمية لمجموعة متنوعة من الأساليب الإحصائية المستخدمة في عدد من المجالات المعرفية على سبيل المثال إدارة الأعمال.

أَمْلِكُ مِثْرًا

المقدمة

أسهمت الابتكارات التكنولوجية المتسارعة والتقنيات المتطورة في أغلب شؤون الحياة اليومية إلى تغيير المفاهيم التقليدية لأمن المعلومات، وفي ظل التزايد الهائل لهذه التكنولوجيا أدى إلى ظهور تحدٍ يواجه المجتمع وهو التهديدات الالكترونية، منها الابتزاز والنصب والاحتيال الالكتروني، الأمر الذي استدعى تطور مفاهيم واستراتيجيات جديدة تتلاءم مع هذه التهديدات منها مفهوم الأمن السيبراني الذي يشير إلى النهج والاجراءات المرتبطة بعمليات ادارة المخاطر الامنية التي تتبعها المنظمات والدول لحماية السرية والنزاهة وتوافر البيانات والاصول المستخدمة في الفضاء الالكتروني، يتضمن المفهوم المبادئ التوجيهية والسياسات ومجموعة الضمانات والتقنيات والادوات والتدريب لتوفير افضل حماية لحالة البيئة الالكترونية ومستخدميها.

ولأهتمام الباحثين في علم الإدارة بشكل خاص بمفهوم أداء المنظمة والذي ينصب على المخرجات التي تسعى المنظمة لتحقيقها، وهو مفهوم يعكس كلاً من الأهداف والوسائل اللازمة لتحقيق المخرجات ذات القيمة التي ينتجها النظام المتمثلة بالأعمال التي تقوم من خلالها المنظمة بتوظيف الموارد والإمكانيات المتاحة لديها والتي يترتب عليها كفاءة وفاعلية المنظمة.

سعى الباحث لبيان العلاقة بين الأمن السيبراني ودوره في أداء المنظمة عن طريق وصف متغيراته وتشخيصها وتقديم بعض التوصيات للشركة عينة البحث.

وعلى ما تقدم جرى تصميم مخطط فرضي يُحدد طبيعة العلاقة بين المتغير المُستقل (الأمن السيبراني) والمتغير التابع (أداء المنظمة) على أساس فرضيتان رئيسيتان وجرى تحليل البيانات التي جمعت من اجابات الافراد عينة البحث.

تضمن البحث أربعة فصول إذ احتوى الفصل الأول على مبحثين، الأول منه حُصص لمنهجية البحث ووصف مجتمع وعينة البحث، والمبحث الثاني تضمن بعض الدراسات السابقة المتعلقة بمتغيرات البحث، وشمل الفصل الثاني على مبحثين، تناول الأول الجانب النظري للأمن السيبراني، في حين عرض المبحث الثاني الجانب النظري لأداء المنظمة، في حين تناول الفصل الثالث ثلاثة مباحث، في الأول جرى استعراض وصف محاور الاستبانة وبيان صدق وثبات المقياس، والمبحث الثاني تضمن التحليل الاحصائي لنتائج الاستبانة باستخدام البرامج (Microsoft Excel 2013 و SPSS V.26) واستخراج المتوسطات وشدة الاجابة والنحرافات لأبعاد المتغيرين المستقل (الأمن السيبراني) والتابع (أداء المنظمة) على شكل جداول

تحتوي على نتائج كل بعد على حدة، والمبحث الثالث وضح اختبار فرضيات البحث الرئيسية وعلاقة الارتباط والتأثير بين المتغيرين موضوع البحث.

اختتم البحث بالفصل الرابع بالاستنتاجات والتوصيات وتكون من مبحثين اساسيين، الاول كان مجموعة من الاستنتاجات التي توصل إليها الباحث، اما المبحث الثاني كان عبارة عن مجموعة من التوصيات الضرورية لشركة عينة البحث.

الفصل الأول

منهجية البحث وبعض الدراسات السابقة السابقة

المبحث الأول: منهجية البحث

المبحث الثاني: بعض الدراسات السابقة

الفصل الأول

منهجية البحث وبعض الدراسات السابقة

تمهيد

سوف يقوم الباحث في هذا الفصل بتقديم فكرة عن مضمون البحث، وقد تم تقسيم الفصل إلى مبحثين، المبحث الأول يتناول منهجية البحث من خلال ذكر مشكلة البحث والتساؤلات التي تعكس المشكلة والأهداف والأهمية وبيان فرضيات البحث والمخطط الفرضي للبحث ووصف كل من مجتمع وعينة البحث وذكر حدود البحث وطرق جمع البيانات والاساليب الاحصائية التي سيعتمدها الباحث في التحليل، أما المبحث الثاني فسيتم خلاله ذكر بعض الدراسات السابقة التي ذكرت متغير الأمن السيبراني أو متغير أداء المنظمة.

المبحث الاول

منهجية البحث

1. مشكلة البحث

أولت العديد من منظمات الأعمال المعاصرة اهتمامًا بالغًا بالأمن السيبراني إذ يُعد من الضرورة الاهتمام بأبعاده وأثره في عدد من المتغيرات ومنها أداء المنظمة. وتواجه المنظمات العراقية مُشكلة تتمثل في محدودية تطبيق الأمن السيبراني والاستفادة منه بشكل فاعل في منظماتها، وفق هذا المنظور تمثلت مشكلة البحث لمحاولة الاجابة عن التساؤلات التالية:

أ. هل تتبنى الشركة عينة البحث تطبيقات الأمن السيبراني وتستثمرها في دعم اعمالها؟

ب. إلى اي مدى يؤثر الأمن السيبراني في أداء الشركة عينة؟

ج. ما ابرز الاجراءات التي تقوم بها ادارة الشركة لتفعيل ممارسات الأمن السيبراني في تعزيز مستوى الأداء التنظيمي فيها؟

2. أهمية البحث

تتبع أهمية البحث من الآتي:

- أ. تسليط الضوء على تطبيقات الأمن السيبراني المعتمدة في الشركة عينة البحث.
- ب. الكشف عن مستوى الأداء للشركة عينة البحث.

- ج. التعريف بمستوى تأثير عامل استخدام الأمن السيبراني في دعم وتحسين مستوى الأداء للشركة عينة البحث.
- د. لفت انظار الإدارات إلى أهمية استثمار تطبيقات الأمن السيبراني لتعزيز أداء المنظمة فيها بما ينعكس بشكل ايجابي على مستوى الخدمات التي تقدمها.

3. أهداف البحث

يهدف البحث لتحقيق الآتي:

- أ. الوقوف على العقبات التي تواجه الشركة عينة في مجال توظيف تطبيقات الأمن السيبراني لدعم الأداء التنظيمي فيها.
- ب. تحديد الدور الذي يشغله متغير الأمن السيبراني في تعزيز أداء المنظمة للمنظمات بشكل عام ومنها المنظمات الخدمية.
- ج. التعريف بابرز العوامل أو العقبات التي تؤثر في مجال توظيف الأمن السيبراني لرفع مستوى الأداء للشركة عينة والذي سينعكس بشكل ايجابي على الخدمات المقدمة فيها.
- د. التوصل إلى بعض النتائج والتوصيات التي تسهم في تعزيز استخدام الأمن السيبراني في دعم أداء الشركة عينة البحث.

4. فرضيات البحث

أ. الفرضية الرئيسية الأولى (H0)

تنص الفرضية الأولى: (لا توجد علاقة ارتباط ذات دلالة معنوية بين الأمن السيبراني بأبعاده وأداء المنظمة بأبعاده) مقابل الفرضية البديلة H1: (توجد علاقة ارتباط ذات دلالة معنوية بين الأمن السيبراني بأبعاده وأداء المنظمة بأبعاده)، ولقد تفرعت عن الفرضية الرئيسية أعلاه ثلاث فرضيات فرعية كالتالي:

أولاً: الفرضية الفرعية الأولى

- H0: لا توجد علاقة ارتباط ذات دلالة معنوية بين السرية وأداء المنظمة بأبعاده.
- H1: توجد علاقة ارتباط ذات دلالة معنوية بين السرية وأداء المنظمة بأبعاده.

ثانياً: الفرضية الفرعية الثانية

- H0: لا توجد علاقة ارتباط ذات دلالة معنوية بين الخصوصية وأداء المنظمة بأبعاده.
- H1: توجد علاقة ارتباط ذات دلالة معنوية بين الخصوصية وأداء المنظمة بأبعاده.

ثالثاً: الفرضية الفرعية الثالثة

- H0: لا توجد علاقة ارتباط ذات دلالة معنوية بين التعزيز وأداء المنظمة بأبعاده.
- H1: توجد علاقة ارتباط ذات دلالة معنوية بين التعزيز وأداء المنظمة بأبعاده.

ب. الفرضية الرئيسة الثانية (H0)

تنص الفرضية الرئيسة الثانية: (لا توجد علاقة تأثير ذات دلالة احصائية للأمن السيبراني في أداء المنظمة) مقابل الفرضية البديلة H1: (توجد علاقة تأثير ذات دلالة معنوية للأمن السيبراني في أداء المنظمة)، ولقد تفرعت عن الفرضية الرئيسة أعلاه ثلاث فرضيات فرعية حسب الآتي:

أولاً: الفرضية الفرعية الأولى

- H0: لا توجد علاقة تأثير ذات دلالة معنوية بين السرية وأداء المنظمة.
- H1: توجد علاقة تأثير ذات دلالة معنوية بين السرية وأداء المنظمة.

ثانياً: الفرضية الفرعية الثانية

- H0: لا توجد علاقة تأثير ذات دلالة معنوية بين الخصوصية وأداء المنظمة.
- H1: توجد علاقة تأثير ذات دلالة معنوية بين الخصوصية وأداء المنظمة.

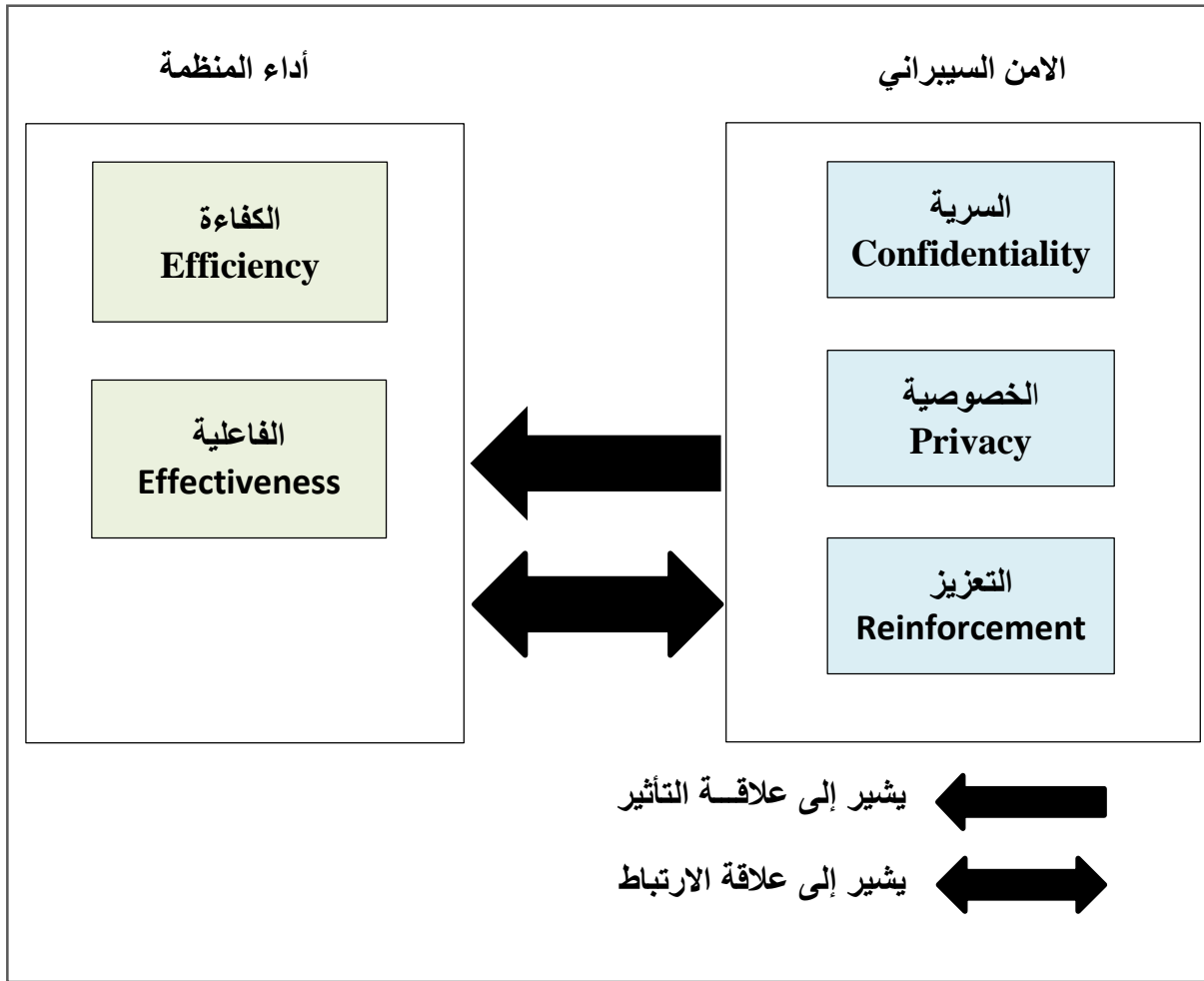
ثالثاً: الفرضية الفرعية الثالثة

- H0: لا توجد علاقة تأثير ذات دلالة معنوية بين التعزيز وأداء المنظمة.
 - H1: توجد علاقة تأثير ذات دلالة معنوية بين التعزيز وأداء المنظمة.
- وسيقوم الباحث باختبار الفرضيات الرئيسة والفرعية المنبثقة عنها في المحور التطبيقي للبحث.

5. مخطط البحث الفرضي

جرى تصميم مخطط فرضي للبحث الحالي لتوضيح ترابط العلاقات المنطقية بين متغيرات البحث عن طريق مشكلة البحث وأهدافه وبجانبه النظري والتطبيقي.

- أ. المتغير المستقل: الأمن السيبراني (x) وابعاده (السرية (x1)، الخصوصية (x2) والتعزيز (x3)).
- ب. المتغير المعتمد: أداء المنظمة (y) وابعاده (الكفاءة (y1) والفاعلية (y2)) والشكل (1) يوضح المخطط الفرضي للبحث.



الشكل (1) المخطط الفرضي للبحث

المصدر: إعداد الباحث

6. حدود البحث

تتمثل حدود البحث الحالي بالآتي:

أ. الحدود المكانية: شركة إيرثلنك (المقر العام) في بغداد.

ب. الحدود الزمانية: (2022/7/15) لغاية (2022/10/15).

7. مجتمع وعينة البحث واختيارها:

أ. اختيار مجتمع البحث:

تم تحديد مجتمع الدراسة بالافراد العاملين في المقر الرئيسي لشركة إيرثلنك في بغداد، وهي احدى شركات الانترنت الرائدة في العراق، عملت كمجهز لخدمات الإنترنت سنة 2005، وتعمل الآن بتزويد خدمات الإنترنت للمنازل، والشركات، والمؤسسات الحكومية.

وتُعد اليوم أكبر مجهز لخدمات الإنترنت في العراق، إذ تغطي شبكتها 15 محافظة عراقية، في ضوء طبيعة عمل الشركة جرى اختيارها لإيجاد علاقة التأثير والارتباط بين متغيرات البحث.

ب. وصف عينة البحث:

أ. تم اختيار عينة قصدية من مختصي تكنولوجيا المعلومات العاملين في المقر الرئيسي لشركة ايرثلنك في بغداد والبالغ عددهم (40 مختصاً) من مجتمع البحث والبالغ (205) من مختلف الاختصاصات، إذ تم اختيار هذه العينة كون اختصاصاتهم قريبة من طبيعة متغير الأمن السيبراني، لما يتطلب من دقة في الإجابة.

ب. وزعت استمارة الاستبانة المعدة لهذا البحث من قبل الباحث إلكترونياً على العينة لمعرفة آرائهم، إذ جرت الإجابة عليها بواقع (40) استمارة صالحة للتحليل.

جدول (1) وصف عينة البحث

ت	الوصف	الفئة	التكرار	النسبة المئوية
1.	النوع الاجتماعي	ذكور	31	77%
		اناث	9	23%
		المجموع	40	100%
2.	الفئة العمرية	25-18	14	35%
		35-26	20	50%
		45-36	6	15%
		55-46	0	0%
		55 فأكثر	0	0%
		المجموع	40	100%
		3.	التحصيل الدراسي	بكالوريوس
دبلوم عالي	0			0%
ماجستير	10			25%
دكتوراه	0			0%
المجموع	40			100%
4.	سنوات الخدمة	أقل من 5 سنوات	37	92%
		5 سنوات فأكثر	3	8%
		المجموع	40	100%
5.		1	13	32%

25%	10	2	عدد دورات الأمن السيبراني لـ 3 سنوات الاخيرة
20%	8	3	
10%	4	4	
13%	5	5 فأكثر	
100%	40	المجموع	

المصدر: اعداد الباحث بالإعتماد على مخرجات الاستبانة.

من الجدول رقم (1) نلاحظ ما يلي:

1. **النوع الاجتماعي:** يتضح ان النسبة الاكبر من عينة البحث كانت من الذكور بنسبة 77%، والاناث بنسبة 23%، وهذا يعود إلى طبيعة العمل التخصصي في مجال الأمن السيبراني وتكنولوجيا المعلومات والذي عموماً تكون فيه نسبة الرجال أكثر من النساء.
2. **الفئة العمرية:** يتضح بأن النسبة الأكبر من عينة الدراسة للفئة العمرية كانت عند (26-35) سنة بنسبة (50%)، أما أقل نسبة فكانت عند الفئتين الاخيرة من (46 فأكثر) سنة وبنسبة (0%)، وهذا يشير ان المنظمة المبحوثة تركز على العناصر الشابة للعمل.
3. **التحصيل الدراسي:** تبين أن النسبة الأكبر من عينة البحث كانت عند شهادة (البكالوريوس) بنسبة (75%) أما أقل نسبة فكانت عند المؤهلات (اعدادية، دبلوم فني، دبلوم عالي ودكتوراه) وبنسبة (0%)، هذا يدل على ان المنظمة المبحوثة تعتمد على حاملي شهادات البكالوريوس فأعلى والذي يعكس اهتمام المنظمة بالتحصيل العلمي من خريجي الكليات لديها.
4. **سنوات الخدمة:** اتضح أنّ النسبة الأكبر من عينة البحث كانت عند (أقل من 5 سنوات) بنسبة (92%) اما الأقل كانت عند عدد سنوات (5 فأكثر) بنسبة (8%) ويعزو الباحث ذلك إلى أن غالبية عينة البحث من حديثي التوظيف الذين لديهم الفاعلية بالعمل والسعي للارتقاء في الوظيفة.
5. **عدد دورات الأمن السيبراني:** تبين من نتائج الاستبانة إن جميع عينة البحث خضعوا لدورات تدريبية تخصصية في مجال عملهم، لتنفيذ المهام المنوطة بهم، مما يدل على اهتمام الشركة بمجال الأمن السيبراني.

8. منهج البحث

اعتمد الباحث على المنهج التحليلي في البحث.

9. أدوات جمع البيانات

لغرض إجراء البحث والتوصل إلى النتائج النهائية اعتمد الباحث الأدوات الآتية:

أ. **الجانب النظري:** تم الحصول على المعلومات المتعلقة بموضوعي البحث (الأمن السيبراني واداء المنظمة) من الكتب والرسائل والاطاريح الجامعية، والمقالات وباللغات العربية والاجنبية من المكتبات المتخصصة وشبكة الانترنت.

ب. **الجانب العملي:** تمثل الاستبانة أداة البحث لجمع البيانات الخاصة بالجانب العملي لمتغيري البحث، إذ عدت استبانة مكونة من ثلاثة محاور (ملحق رقم 3):

أ. **المحور الاول:** وصف عينة البحث، المتضمنة معلومات تعريفية مثل (النوع الاجتماعي، الفئة العمرية، التحصيل الدراسي، سنوات الخدمة وعدد الدورات التخصصية في مجال الأمن السيبراني).

ب. **المحور الثاني:** الفقرات الخاصة بالمتغير المستقل للبحث (الامن السيبراني) والتي ضمت (18) فقرة، وزعت على ثلاثة أبعاد بواقع (6) فقرات لكل بعد، جرى اعدادها بناءً على مقياس دراسة (نخيلان، 2020).

ج. **المحور الثالث:** الفقرات الخاصة بالمتغير التابع (أداء المنظمة) التي ضمت (8) فقرات، وزعت على بُعدين بواقع (4) فقرات لكل بعد، تم اعدادها بالاعتماد على مقياس دراسة (الموسوي، 2018).

10. الاساليب الاحصائية

تم اعتماد الاساليب الاحصائية الآتية:

- اعتماد مقياس (likert) خماسي الدرجات كونه يتسم بالوضوح والدقة.
- النسب المئوية والتكرارات.
- الوسط الحسابي.
- الانحراف المعياري.
- شدة الاجابة.
- معامل الارتباط.
- معامل التأثير.
- معامل Cronbach's Alpha.
- معامل الاختلاف.
- معامل الانحدار الخطي البسيط.

المبحث الثاني

بعض الدراسات السابقة

توطئة

يتناول هذا المبحث بعض الدراسات التي تطرقت لأحدى متغيري البحث (الأمن السيبراني أو أداء المنظمة)، وذلك لقلّة الدراسات (حسب اطلاع الباحث) التي ذكرت المتغيرين معاً، لذا سيجري ذكر دراسات تناولت احد متغيري البحث من الأحدث إلى الأقدم:

1. بعض الدراسات السابقة التي تناولت متغير الأمن السيبراني

أ. الدراسات العربية:

جدول (2) الدراسات العربية السابقة الخاصة بمتغير الأمن السيبراني

دراسة (منصور، 2021)	
تأثير الأمن السيبراني على الرقابة الداخلية وانعكاسها على الوحدة الاقتصادية – دراسة استطلاعية لأراء عينة من المدققين والمحاسبين في وزارة التعليم العالي والبحث العلمي	عنوان الدراسة
بحث منشور في مجلة.	مستوى الدراسة
توضيح أهمية الامن السيبراني من خلال تأثيره على الرقابة الداخلية وقيمة الوحدة الاقتصادية.	هدف الدراسة
الأمن السيبراني (الاستراتيجية، العمليات والاجراءات، الحماية السرية والخصوصية، الأمن المنطقي والمخاطر اسيرانية)، قيمة الوحدة الاقتصادية والاطر الحديثة للرقابة.	أبعاد الدراسة
بلغ حجم مجتمع الدراسة (130) مدققاً ومحاسباً ولتمثيل المجتمع بطريقة علمية جرى استعمال الطريقة الاحصائية (معادلة ستيفن ثامبسون) لضبط حجم العينة التي بلغت (98) مستجيباً في وزارة التعليم العالي والبحث العلمي.	المجتمع والعينة
دلت النتائج الى تبني الوحدة الاقتصادية آلية عمل التقييم الذاتي للرقابة الداخلية الالكترونية ومجالات الأمن السيبراني لتقييم المخاطر السيبرانية للارتقاء بمستويات الحماية السيبرانية وكذلك تكامل عناصر الرقابة الداخلية في ظل اطار	أبرز النتائج

عمل COBIT5 وضرورة تطبيقها بصورة مجتمعة من أجل تحقيق أهداف الرقابة.	
الإحصاء الوصفي والاستدلالي.	الأساليب الإحصائية
دراسة (نخيلان، 2020)	
دور الأمن السيبراني في تحقيق جودة الخدمات الإلكترونية بعمادة تقنية المعلومات بجامعة الملك عبد العزيز "دراسة ميدانية"	عنوان الدراسة
رسالة ماجستير في الإدارة العامة.	مستوى الدراسة
<ul style="list-style-type: none"> - الكشف والتعرف على أساسيات الأمن السيبراني (السرية والخصوصية والتعزيز) في جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز. - التعرف على دور عمل الأمن السيبراني في التعزيز الأمني للخدمات الإلكترونية. 	هدف الدراسة
السرية، الخصوصية، التعزيز وجودة الخدمات الإلكترونية.	أبعاد الدراسة
يتكون مجتمع الدراسة من موظفين وموظفات عمادة تقنية المعلومات بجامعة الملك عبد العزيز والبالغ (221)، إذ طبقت الدراسة على عينة قصدية مقدارها (150) موظفًا وموظفة.	المجتمع والعينة
<ul style="list-style-type: none"> - يمارس العاملون في عمادة تقنية المعلومات بجامعة الملك عبد العزيز بعدي السرية والخصوصية بدرجة مرتفعة، وبعد التعزيز بدرجة مرتفعة جدًا. - جودة الخدمات الإلكترونية في عمادة تقنية المعلومات تتميز بدرجة مرتفعة من وجهة نظر العاملين. 	أبرز النتائج
تم استخدام العديد من الأساليب الإحصائية باستخدام الحزم الإحصائية للعلوم الاجتماعية (SPSS) كـ (التكرارات والنسب المئوية، المتوسط الحسابي، الانحراف المعياري، اختبار ألفا كرونباخ، معامل الارتباط بيرسون واختبار أنوفا).	الأساليب الإحصائية

دراسة (السيد، 2021)	
عنوان الدراسة	الأمن السيبراني وعلاقته بالمضمون الإعلامي في ظل رؤية مصر 2030
مستوى الدراسة	بحث منشور في مجلة.
هدف الدراسة	<ul style="list-style-type: none"> - شرح مفهوم الأمن السيبراني والتهديدات الإلكترونية ومخاطر استخدام الانترنت وجرائم الاتصال عبر الانترنت ذات الصلة بوسائل الإعلام. - توضيح دور المضمون الإعلامي في تحقيق الوعي الأمني واثار المضمون الإعلامي في تحقيق الأمن الفكري. - تحليل اخلاقيات الاتصال الإعلامي عبر الإنترنت وعلاقتها بتحقيق الأمن السيبراني.
أبعاد الدراسة	- احادي البعد.
المجتمع والعينة	مجتمع الدراسة اساتذة جامعيين في تخصص الإعلام وتكنولوجيا الاتصال وتقنية المعلومات والأمن السيبراني بكليتي الإعلام والهندسة وكانت العينة قصدية متكونة من (32) أستاذًا جامعيًا ضمن التخصصات السابقة.
أبرز النتائج	يعد الأمن السيبراني أمرًا بالغ الأهمية بشكل خاص لحماية محتوى المضمون الإعلامي الذي تنتجه المؤسسات الإعلامية والترفيهية، لبناء الجماهير التي تدعم أنموذج الأعمال الإعلامية في ظل رؤية مصر 2030.
الأساليب الاحصائية	استخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS) في تحليل البيانات وفقًا للأساليب الاحصائية (معامل ألفا كرونباخ، التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية).

ب. الدراسات الأجنبية:

جدول (3) الدراسات الأجنبية السابقة الخاصة بمتغير الأمن السيبراني

دراسة (Kosutic, 2021)	
عنوان الدراسة	The Impact of Cybersecurity on Competitive Advantage تأثير الامن السيبراني على الميزة التنافسية

<p>أطروحة دكتوراه في إدارة الأعمال.</p>	<p>مستوى الدراسة</p>
<p>تهدف هذه الأطروحة إلى استكشاف العناصر اللازمة لتنفيذ الأمن السيبراني وإدارته في المنظمة، وكذلك استكشاف كيف يمكن للأمن السيبراني أن يسهم في الميزة التنافسية للمنظمة.</p>	<p>هدف الدراسة</p>
<p>الأمن السيبراني (القدرات التشغيلية، القدرات الديناميكية).</p>	<p>أبعاد الدراسة</p>
<p>ثلاث جولات من المقابلات شبه المنظمة مع ضباط الأمن والمديرين التنفيذيين والاستشاريين وتكنولوجيا المعلومات (IT) مديرين من شركات في 10 دول، و7 صناعات، من مجالات الفضاء، والعلوم الحيوية، والتصنيع الكيميائي، والمالية، وتجهيز الأغذية، وتكنولوجيا المعلومات، والصناعات الأمنية، وأربعة مناصب مختلفة، وتكون مجتمع الدراسة من 19 شخصًا وتم اعتماد 15 عينة من خلال المقابلات.</p>	<p>المجتمع والعينة</p>
<p>- هناك حاجة إلى نهج شامل لإدارة الأمن السيبراني من خلال نظام اجتماعي تقني يوازن بين الجوانب الاستراتيجية والتنظيمية والمخاطر والتكنولوجيا والأشخاص.</p> <p>- الامتثال للمتطلبات المختلفة، يمكن للمنافسين محاكاة الامتثال بسهولة لأنه يعتمد على القدرات التشغيلية، من خلال تطوير قدرات ديناميكية محددة للأمن السيبراني، يمكن للشركات تحقيق قيمة استراتيجية يصعب تقليدها، ومن ثم تحقيق ميزة تنافسية مستدامة.</p>	<p>أبرز النتائج</p>
<p>تم تحليل النصوص من خلال المقابلات شبه المنظمة الخاصة بمعرفة الإجابات على سؤالي البحث: 1. ما هي العناصر الحاسمة لتنفيذ وإدارة الأمن السيبراني بنجاح في المنظمة؟ 2. كيف يؤثر الأمن السيبراني على الميزة التنافسية للشركة؟ من خلال ثلاث جولات من المقابلات، وعرض تفاصيل إحصائية حول عدد الأشخاص الذين تمت مقابلتهم، والمسميات الوظيفية، والبلدان، ومجالات عملهم، ومعدلات الاستجابة.</p>	<p>الأساليب الإحصائية</p>

دراسة (Onumo, 2020)	
A Behavioural Compliance Framework for Effective Cybersecurity Governance and Practice	عنوان الدراسة
إطار الامتثال السلوكي لحوكمة وممارسة فعالة للأمن السيبراني	
أطروحة دكتوراه في الفلسفة.	مستوى الدراسة
دراسة دور الثقافة في تطوير الأمن السيبراني وممارسة الأمن التنظيمي.	هدف الدراسة
الآليات التي تؤدي إلى ممارسات أمنية فردية تنظيمية، تقييم ثقافة المنظمة، عنصر التحكم التنظيمي القيادي والجزء الديموغرافي.	أبعاد الدراسة
تكون المجتمع من 300 موظف لثلاث مؤسسات لتكنولوجيا المعلومات في القطاع العام في نيجيريا ومثله عينة من 122 موظفًا.	المجتمع والعينة
النتائج في هذا البحث لها آثار على صانعي السياسات والممارسين من خلال رفع أهمية الديناميكيات الثقافية والمعرفية من خلال تعزيز الوضوح التشغيلي في ممارسة الأمن التنظيمي وتقديم فرصة لتطوير حل إبداعي وقوي لتحدي الأمن التنظيمي بما يتماشى مع الخصائص الثقافية.	أبرز النتائج
الاحصاء الوصفي.	الأساليب الاحصائية
دراسة (Uwakweh, 2020)	
Cybersecurity in the Retail Industry: Third Party Implications	عنوان الدراسة
الأمن السيبراني في صناعة البيع بالتجزئة: الآثار المترتبة على الطرف الثالث	
رسالة ماجستير في العلوم.	مستوى الدراسة
معرفة شركات البيع بالتجزئة مخاطر الأمن السيبراني والتدابير الأمنية المناسبة لحماية نفسها وزبائنهم.	هدف الدراسة
- احادي البعد.	أبعاد الدراسة
تم النظر فقط في انتهاكات بيانات البيع بالتجزئة من السنوات 2013 – 2018 لمجموعة من الصناعات.	المجتمع والعينة

<p>- عندما تحدث خروقات للبيانات وتشاركه أطراف ثالثة، فإن فقدان السجلات يميل إلى أن يكون أعلى مما لو كان خرقاً مباشراً ضد شركة.</p> <p>- إن صناعة البيع بالتجزئة بشكل عام تميل إلى الحصول على أمان أفضل ومعدلات نجاح أقل لخروقات البيانات بعد حدوث انتهاك رئيس.</p>	<p>أبرز النتائج</p>
<p>تحليل البيانات الثانوية.</p>	<p>الأساليب الاحصائية</p>

2. بعض الدراسات السابقة التي تناولت متغير أداء المنظمة أ. الدراسات العربية:

جدول (4) الدراسات العربية السابقة الخاصة بمتغير أداء المنظمة

دراسة (منسي، 2022)	
<p>تأثير الحكومة الالكترونية في أداء المنظمات: دراسة تحليلية لآراء عينة من ضباط وموظفي مديرية المرور العامة/ مديرية تسجيل المركبات وإجازات السياقة</p>	<p>عنوان الدراسة</p>
<p>الدبلوم العالي (معادل للماجستير) في التخطيط الاستراتيجي الأمني.</p>	<p>مستوى الدراسة</p>
<p>بيان تأثير "الحكومة الإلكترونية" في أداء المنظمات عبر ابراز دور مديرية المرور العامة (مديرية تسجيل المركبات واجازات السياقة) في مجال التحول باتجاه تحقيق متطلبات "الحكومة الالكترونية".</p>	<p>هدف الدراسة</p>
<p>تحسين كفاءة العمل، التركيز على المستفيدة من الخدمة، زيادة مشاعر رضا العاملين والالتزام التنظيمي.</p>	<p>أبعاد الدراسة</p>
<p>تكون مجتمع الدراسة من (558) من الضباط والموظفين وتم اختيار عينة قصدية منهم البالغة (142).</p>	<p>المجتمع والعينة</p>
<p>- إن المنظمة المبحوثة لديها تطبيق لمتطلبات الحكومة الالكترونية بشكل متوسط على مستوى تطبيق المهام والوظائف المناطة بها.</p> <p>- إن المنظمة المبحوثة تمتلك رصيذاً جيداً من القدرات البشرية المؤهلة في مضمار العمل التقني.</p>	<p>أبرز النتائج</p>
<p>كلاً من (التحليل العائلي التوكيدي، اختبار الفا كرونباخ، الوسط الحسابي، الانحراف المعياري، معامل ارتباط بيرسون ونمذجة المعادلة الهيكلية).</p>	<p>الأساليب الاحصائية</p>

دراسة (غانم، 2021)	
عنوان الدراسة	تأثير جودة التدقيق الداخلي لنظام إدارة الجودة في الأداء التنظيمي – دراسة حالة في شركة مصافي الوسط
مستوى الدراسة	الدبلوم العالي في إدارة الجودة.
هدف الدراسة	بيان أهمية عملية التدقيق الداخلي لنظام إدارة الجودة كونه مطلبًا أساسيًا يستوجب على المنظمات التي تطبق نظام إدارة الجودة (ISO-9001) القيام به.
أبعاد الدراسة	رضا الزبون، مطابقة المنتجات للمتطلبات، أداء العملية والتحسين المستمر.
المجتمع والعينة	تمثل مجتمع البحث شركة مصافي الوسط التابعة لوزارة النفط، أما عينة البحث فتم اختيار (قسم المزج وأوعية التعبئة) من الشركة المبحوثة.
أبرز النتائج	<ul style="list-style-type: none"> - عدم وجود علاقة ارتباط بين عملية التدقيق الداخلي لنظام إدارة الجودة والاداء التنظيمي. - عملية التدقيق الداخلي تجري وفقًا للمعايير المطلوبة في المواصفات القياسية. - الشركة تهتم بمؤشرات الأداء التنظيمي وتحافظ على تطبيقها.
الأساليب الإحصائية	اعتمد الباحث في بحثه على أسلوب دراسة الحالة واعتمد وثائق الشركة بيانات موثقة ومعتمدة، واستخدم الأساليب الإحصائية (معامل ارتباط بيرسون، المتوسطات الحسابية) واستخرجها بواسطة برنامج الحزم الإحصائية للعلوم الاجتماعية (SPSS).
دراسة (الموسوي، 2018)	
عنوان الدراسة	دور استراتيجية التسويق في تحسين الأداء المنظمي للمستشفيات الأهلية
مستوى الدراسة	بحث منشور في مجلة.
هدف الدراسة	تحديد طبيعة دور استراتيجية التسويق واثرها في تحسين الاداء التنظيمي في المستشفيات الأهلية.
أبعاد الدراسة	الفاعلية، الكفاءة.

اختير القطاع الصحي كمجتمع للجانب العملي واختيرت مستشفى الخيال الأهلية كميدان للتطبيق، وتم اختيار عينة البحث بطريقة العينة العشوائية البسيطة والمكونة من (25) شخصاً.	المجتمع والعينة
- وجود علاقة ارتباط وتأثير ذات دلالة معنوية لاستراتيجية التسويق في تحسين الاداء التنظيمي.	أبرز النتائج
تم استخدام البرنامج الاحصائي الجاهز (SPSS) وبرنامج (Excel) في ادخال وتحليل بيانات البحث، وكذلك معامل التكرار، الوسط الحسابي، الانحراف المعياري، معامل الاختلاف، معامل الارتباط لسبيرمان، معامل الانحدار الخطي البسيط.	الأساليب الاحصائية

ب. الدراسات الأجنبية:

جدول (5) الدراسات الأجنبية السابقة الخاصة بمتغير أداء المنظمة

دراسة (John, 2022)	
SERVANT LEADERSHIP IMPACT ON ORGANIZATIONAL PERFORMANCE	عنوان الدراسة
تأثير قيادة الخادم على الأداء التنظيمي	مستوى الدراسة
اطروحة دكتوراه في إدارة الأعمال.	هدف الدراسة
تهدف هذه الدراسة البحثية النوعية على نهج القيادة المعاصرة والقيادة الخادمة وتأثيرها على الأداء التنظيمي.	أبعاد الدراسة
احادي البعد.	المجتمع والعينة
استندت بشكل أساسي إلى بيانات المقابلات من 26 فرداً عبر خمس شركات في قطاع النفط والغاز، وبيانات مسح من 51 مشاركاً، ومراجعة للوثائق المتاحة للعاملين.	أبرز النتائج
- القيادة الخادمة هي أسلوب قيادة فعال يمكن أن يؤثر بشكل إيجابي على الأداء التنظيمي من منظور الثقافة التنظيمية، ومشاركة الموظفين، واستراتيجية العمل.	

<p>- يؤثر القادة الخدم على هذا التأثير من خلال تمكين الموظفين ومحاسبتهم، وخلق شعور بالمجتمع داخل مؤسساتهم.</p>	
<p>تضمن تحليل البيانات تطوير نهج منظم وعملية مرنة لفحص البيانات التي جمعت من قبل الباحث باستخدام نهج له خطوات عدة، تتمثل بالترميز أي تعيين رموز أو علامات ليست أكثر من كلمات أو عبارات محددة تتعلق بالعناصر غير القابلة للقياس الكمي (مثل الأحداث والسلوكيات والأنشطة) التي تمثل موضوعاً أو فكرة معينة، واستخدام برامج البحث النوعي، مثل NVivo، في تنظيم البيانات، ومن ثم إنشاء مصفوفة من الفئات المتناقضة وتعيين الأدلة وفقاً للمصفوفة، وبعدها جرى إنشاء عروض مرئية (المخططات الانسيابية) لفحص البيانات.</p>	<p>الأساليب الاحصائية</p>
<p>دراسة (Thilagawathi, 2021)</p>	
<p>EXAMINING AGILE LEADERSHIP STYLE ON ORGANIZATIONAL PERFORMANCE THROUGH THE MEDIATION OF ORGANIZATIONAL CULTURE: A CASE STUDY ON PROFESSIONAL BODIES IN MALAYSIA</p> <p>فحص أسلوب القيادة الرشيق في الأداء التنظيمي من خلال وساطة الثقافة التنظيمية: دراسة حالة عن الهيئات المهنية في ماليزيا</p>	<p>عنوان الدراسة</p>
<p>اطروحة دكتوراه في إدارة الأعمال.</p>	<p>مستوى الدراسة</p>
<p>تبحث هذه الدراسة تأثير أسلوب القيادة الرشيق على الأداء التنظيمي من خلال وساطة الثقافة التنظيمية.</p>	<p>هدف الدراسة</p>
<p>الأداء التنظيمي.</p>	<p>أبعاد الدراسة</p>
<p>تمثل مجتمع الدراسة بالهيئات المهنية المحددة في ماليزيا، العينة تكونت من (75) من رؤساء الإدارات والمديرين.</p>	<p>المجتمع والعينة</p>
<p>أشارت النتائج إلى وجود علاقة كبيرة بين أسلوب القيادة الرشيق والأداء التنظيمي، علاوة على ذلك للثقافة التنظيمية تأثير وسيط بين أسلوب القيادة الرشيق والأداء التنظيمي.</p>	<p>أبرز النتائج</p>

<p>تم استخدام أنموذج المعادلة الهيكلية (SEM) لإجراء التحليل الإحصائي لتحديد العلاقات السببية بين المتغيرات وتأكيد الفرضيات المطورة.</p>	<p>الأساليب الإحصائية</p>
<p>دراسة (Obeed, 2021)</p>	
<p>The quality of institutional performance according to the entrepreneurial management Applied research in the Municipality of Baghdad</p> <p>جودة الاداء المؤسسي حسب ادارة المشاريع البحثية التطبيقية في امانة بغداد</p>	<p>عنوان الدراسة</p>
<p>بحث منشور في مجلة.</p>	<p>مستوى الدراسة</p>
<p>يهدف البحث إلى تحديد دور إدارة المشاريع في تحقيق جودة الأداء المؤسسي في أمانة بغداد من خلال تحديد دور الإدارة بمستوياتها في تحقيق جودة الأداء المؤسسي.</p>	<p>هدف الدراسة</p>
<p>الأداء المالي، العمليات الداخلية، رضا العملاء.</p>	<p>أبعاد الدراسة</p>
<p>يتكون مجتمع البحث من الذين يشغلون مناصب إدارية مسؤولة ضمن مستوى الإدارة العليا والمتوسطة، كما شملت العينة (المديرين العاميين، والمديرين العاميين المساعدين، ومديري الأقسام) في مركز امانة بغداد.</p>	<p>المجتمع والعينة</p>
<p>- أن إدارة المشاريع تؤدي دورًا رئيسًا في جودة الأداء المؤسسي. - ضعف عملية التخطيط للإدارة وعدم وجود رؤية واضحة في الأنشطة وعمل المنظمة المبحوثة.</p>	<p>أبرز النتائج</p>
<p>تحليل البيانات جرى بالاعتماد على طريقة إحصائية (تحليل وصفي) عن طريق استخراج التكرارات والأوزان والوسائل الحسابية والنسب المئوية.</p>	<p>الأساليب الإحصائية</p>

3. مجالات الاستفادة من الدراسات السابقة

من خلال الاطلاع ومراجعة الدراسات السابقة تم الاستفادة منها في بعض المجالات منها:

1. المساعدة في إعداد منهجية البحث الحالي، من خلال التعرف على أسلوب المنهج العلمي المتبع في الدراسات السابقة.

2. أغنت الدراسات السابقة متغيرات البحث الحالي في الجانب النظري.
3. التعرف على نتائج الدراسات السابقة والاستفادة من الاساليب والادوات المستخدمة للوصول إلى أهداف البحث.

4. مميزات البحث الحالي عن الدراسات السابقة

أهم ما ميّز هذا البحث عن البحوث السابقة يمكن توضيحه بالآتي:

1. التعرف على المجالات التي لم تناقشها الدراسات السابقة ومحاولة تقليل الفجوة الخاصة في توضيح تأثير الأمن السيبراني في أداء المنظمة من خلال الجانب النظري بصورة أكثر دقة.
2. يُقدم البحث الحالي مقترحًا يوضح مدى أهمية تبني المنظمة للأمن السيبراني للنهوض بواقعها العملي على المستوى المحلي.
3. اجري البحث الحالي في البيئة العراقية، للتعرف على الأمن السيبراني وأداء المنظمة في الشركة عينة البحث، والتي تعد من الشركات الرئيسية المجهزة لخدمات الانترنت في العراق.
4. يعتبر البحث من الموضوعات الحديثة التي تساهم في تطور وتقديم العلم.

الفصل الثاني

الجانب النظري

المبحث الأول: الأمن السيبراني

المبحث الثاني: أداء المنظمة

الفصل الثاني

الجانب النظري

تمهيد

نظراً لأهمية متغيرات البحث (الأمن السيبراني وأداء المنظمة) سوف يتم التطرق في هذا الفصل إلى هذه المتغيرات بشيء من التفصيل وقد تم تقسيم الفصل إلى مبحثين، المبحث الأول يتناول الجانب النظري للأمن السيبراني، إذ سيتم ذكر نشأة الأمن السيبراني ومفهومه وأهميته ومبررات تبني معايير الأمن السيبراني في المنظمات وأنواعه وتهديداته وكذلك ابعاد الأمن السيبراني.

أما المبحث الثاني فسيتم خلاله عرض جوانب المتغير الثاني وهو أداء المنظمة، إذ سيتم التطرق إلى مفهومه وأهميته ومستويات أداء المنظمات وقياس أداء المنظمة وأبعاد أداء المنظمة.

المبحث الأول

الأمن السيبراني

توطئة

تعتمد المجتمعات الحديثة بشكل متزايد على تكنولوجيا المعلومات المتصلة بالشبكة العالمية، غير أن هذا الاعتماد ترافقه مجموعة من المخاطر الناشئة والمحتملة التي تهدد وبشكل أساسي الشبكة وأمن المعلومات والمجتمع المعلوماتي وأعضائه، إن سوء الاستغلال للشبكات الالكترونية لأهداف إجرامية يؤثر سلباً على سلامة البنى التحتية للمعلومات الحساسة لا سيما على المعلومات الشخصية، الأمر الذي أدى لظهور مفاهيم جديدة رادعة لهذه التهديدات منها مفهوم الأمن السيبراني الذي سنسلط الضوء عليه لما له أهمية للعديد من المنظمات في وقتنا الحاضر.

نشأة الأمن السيبراني

تاريخ الأمن السيبراني لم يبدأ إلا في سبعينيات القرن الماضي، إذ بدء استخدام الهندسة الاجتماعية للحصول على معلومات الكمبيوتر مثل أرقام الهواتف ورموز الكمبيوتر والمعلومات التقنية وأسماء المستخدمين وكلمات المرور للتحايل على نظام البطاقة المثقوبة واستخدامها كوسيلة لركوب الحافلات (Middleton, 2017: 3).

مع ازدياد الهجمات الإلكترونية والتهديدات الجاسوسية في فترة الثمانينيات، ظهرت مصطلحات جديدة مثل فيروسات الحاسوب (Trojan Horse) الذي تم استخدامه بكفاءة لأول مرة في أواخر عام 1989 (Giri, 2006: 1)، خلال الثمانينيات العالم ادرك ضعف أمن أنظمة الكمبيوتر الموجودة آنذاك والبدء في بناء قوانين أمن الكمبيوتر.

في فترة التسعينيات وبسبب دخول خدمة الانترنت في الكثير من المجالات وازدياد عدد المستخدمين للمواقع الإلكترونية، بدأت محاولة كثيرين في تصميم فيروسات أقوى وأشد فعالية، وبالمقابل تكثفت الجهود لتصميم برامج أشد مقاومة للفيروسات و تصميم جدران فائقة الحماية لمكافحة الفيروسات.

أما في فترة القرن الحادي والعشرين وبسبب تضاعف التهديدات وعمليات الاختراق بصورة مُحترفة، فقد دفع هذا الحكومات والدول لاتخاذ العديد من الإجراءات الصارمة مثل سن التشريعات بخصوص هذه الأنواع من الجرائم، وإصدار العديد من الأحكام الجنائية المتعلقة في هذا الخصوص، مع توجه معظم الشركات والمؤسسات لدمج وادخال الذكاء الصناعي لإنشاء جدار أمني عالي الكفاءة لغرض مكافحة الهجمات الفيروسية (Middleton, 2017: 12).

مفهوم الأمن السيبراني

يعد مجال الأمن السيبراني مجالاً متنامياً، ويحظى بقدر كبير من الاهتمام لاستخداماته في المنظمات الخاصة والحكومية، قد يكون مصطلح الأمن السيبراني بالنسبة للكثير مجرد كلمة متخصصة قد لا تعني كثيراً بالنسبة لهم، لذلك يجب تحديد ما تعنيه هذه الكلمة بالضبط من خلال التعريفات في الجدول الآتي:

جدول (6) تعريفات الأمن السيبراني

ت	المصدر	التعريف
1.	(Whitman & Mattford, 2019)	حماية المعلومات المحوسبة وأنظمة المعالجة والبيانات التي تحتويها وتعالجها.
2.	(Rodriguez, 2019)	القدرة على حماية أو الدفاع عن استخدام الفضاء الإلكتروني من الهجمات الإلكترونية.
3.	(Rawass, 2019)	الأدوات والسياسات ونماذج الأمان والاحتياطات الأمنية والاستراتيجيات وتكتيكات إدارة المخاطر والأنشطة والإعداد وأفضل الممارسات والضمان والتقنيات المستخدمة لحماية الغلاف الجوي الإلكتروني والمعاهد وبيانات المستخدم.

مجموعة الأدوات والسياسات والمفاهيم الأمنية والضمانات والمبادئ التوجيهية وأساليب إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمان والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المنظمة والمستخدمين.	(ONUMO, 2020)	.4
الحماية من السرقة أو التلف للأجهزة والخدمات والشبكات بما في ذلك المعلومات الواردة بداخلها.	(مركز الأمن السيبراني الوطني في المملكة المتحدة، 2021)	.5

المصدر: من اعداد الباحث بالاعتماد على الأدبيات

أهمية الأمن السيبراني في المنظمات

يمكن توضيح ابرز فوائد الامن السيبراني من خلال النقاط الآتية (منصور، 2021: 226-228)، (عثماني، 2019: 19):

1. يساعد على تجنب الغرامات والعقوبات

يفرض المشرعون بشكل متزايد تشريعات تحمي أمن وخصوصية البيانات الشخصية التي تجمعها الشركات والمنظمات الخاصة، يمكن أن يؤدي انتهاك هذه القوانين إلى فرض غرامات وعقوبات شديدة، ولكن لدى المنظمات ذات وظائف الامتثال الأمني القوي الفرصة لتجنب هذه المشكلات من خلال تأمين البيانات التي تجمعها بشكل مناسب.

2. حماية سمعة المنظمة

إن تعرض منظمة ما خرق لبياناتها سيضر بسمعتها، وستضطرب الثقة بين المنظمة وزبائنها، فأي حادثة اختراق تتعرض لها المنظمة وتؤدي لتسريب بياناتها الحساسة أو تخريبها ستنقل رسالة واضحة للزبائن بأن هذه المنظمة غير جديرة بالثقة ولا يعمل صانعو القرار بها على اتخاذ الخطوات المناسبة لحماية خصوصيتهم وأمنهم.

3. تعزيز قدرات إدارة البيانات

بالنسبة لمعظم المنظمات العاملة في تقنية المعلومات، يبدأ الحفاظ على الامتثال لمعايير أمن البيانات بتتبع المعلومات الحساسة التي يحتفظون بها حول الزبائن وتطوير القدرات للوصول إلى هذه المعلومات وتعديلها بطريقة مبسطة.

4. تحسين صورة المنظمة

عادة ما تتردد المنظمات التي استثمرت وقتاً ومواردًا كبيرة للحفاظ على الامتثال لإرشادات أمن البيانات الخاصة بالصناعة في الشراكة مع المنظمات التي لم تفعل الشيء نفسه، فالامتثال لمعايير الأمن السيبراني يساعد الآخرين على الإدراك كشريك رائد في الصناعة في مجال الأمن وشريك موثوق في العمل.

5. تعزيز ثقافة المنظمة في أمن المعلومات

تتمتع المنظمات التي تجمع البيانات من عملائها بفرصة فريدة لتعزيز ثقافتها من خلال اعتماد تدابير الامتثال الأمني المتطورة التي تلبّي أو تتجاوز المعايير أو اللوائح المعمول بها وتُظهر قيادة الصناعة في مجال أمن المعلومات، يمكن للمنظمات بناء ثقافة داخلية وهوية خارجية حول الأهمية التي توليها لخصوصية الزبائن وأمنهم، ووضع منظمتهم على أنها تقوم بالشيء الصحيح، وتأخذ الأمن على محمل الجد، وتستثمر في أمن وخصوصية الموظفين والزبائن، وأنها ترى أمان البيانات بأنه مصدر فخر وثقة وليس التزامًا قانونيًا، كما يوصي الخبراء بضرورة تأهيل الملاكات الأمنية في المنظمة من خلال تدريبات العاملين والذين يُعدون أسهل طريقة للولوج إلى النظام من قبل المجرمين الإلكترونيين، حيث تعمل هذه التدريبات على تمكين معارف العاملين حول الحوادث الأمنية والهجمات السيبرانية وكيفية التصرف إزاء هذه المواقف.

6. التوافق الأمني يدعم ضوابط الوصول والمساءلة

يضمن النظام الفعال للامتثال لأمن تقنية المعلومات أن الأفراد الذين لديهم بيانات اعتماد مناسبة فقط يمكنهم الوصول إلى الأنظمة وقواعد البيانات الآمنة التي تحتوي على بيانات الزبائن المهمة، يجب أن تضمن المنظمات التي تطبق أنظمة المراقبة الأمنية أن الوصول إلى تلك الأنظمة يجري مراقبته على مستوى المنظمة، والإجراءات تُسجل داخل النظام إذ يمكن تتبعها إلى أصلها، هذا النوع من المراقبة هو خطوة ضرورية لمنع حدوث خرق للبيانات، ويجب أن تحتفظ المنظمة بقائمة بالأشخاص المعتمدين فيها والذين بإمكانهم الوصول إلى البيانات، وكما يجب مراجعة القائمة بانتظام لحساب تغييرات الدور والحالة بين العاملين، كما يمكن للمنظمات دمج إزالة التصاريح الأمنية في العمليات الخارجية لجميع العاملين في الشركة.



الشكل (2) فوائد الأمتثال لمعايير الأمن السيبراني في المنظمات

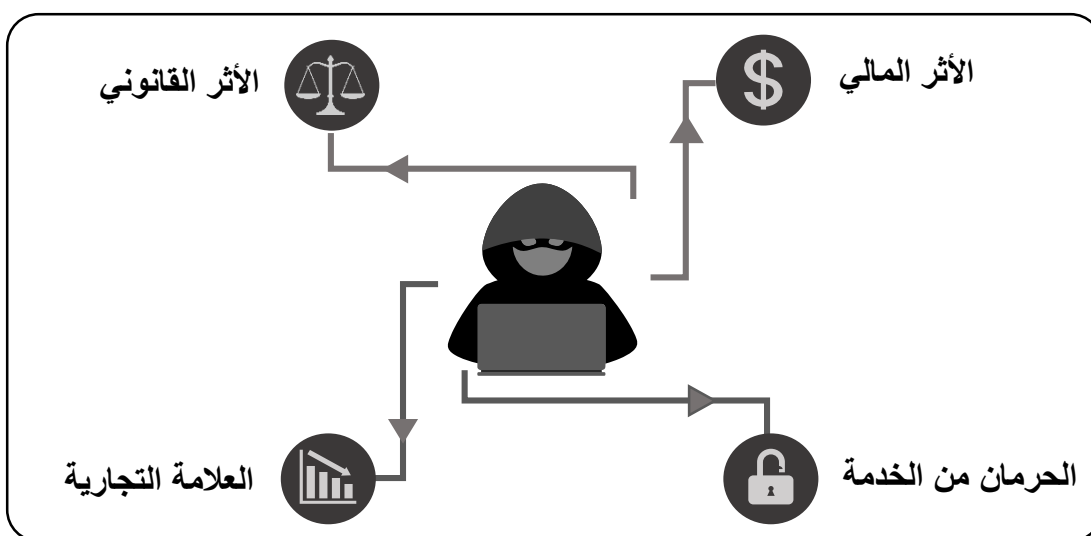
المصدر: رؤى حمود، مجموعة ريناد المجد لتقنية المعلومات، 6 مزايا خفية يقدمها الامتثال لمعايير الأمن السيبراني، 2022، <https://www.rmg-sa.com/> الامتثال-لمعايير-الأمن-السيبراني/

مبررات تبني معايير الأمن السيبراني في المنظمات

يشكل تقدم التكنولوجيا وحقيقة أنّ عدد المتسللين يتزايد ومهاراتهم تتقدم مما يسبب تهديدًا كبيرًا للمنظمات بمختلف أنواعها، وأهمية الأمن السيبراني للمنظمات يكمن بشكل أفضل من خلال معرفة آثار الهجوم الإلكتروني عليها والمتمثلة بالآتي (Kosutic, 2021: 159-160):

1. **الأثر المالي:** غالبًا ما تخسر الشركات التي تتعرض لهجمات إلكترونية كثيرًا من الأموال في شكل مدفوعات فدية أو انخفاض قيمة الشركة أو تحويلات مالية غير معتمدة أو انخفاض في المبيعات، كذلك تكلفة التحقيق في الهجوم والتي تتطلب كثيرًا من العمل الذي يجب القيام به بعناية، وفي معظم الأحيان تقوم الشركة المتعرضة لهجمات بتوظيف شركة استشارية متخصصة في التحقيقات الجنائية الإلكترونية لتحليل الأدلة.
2. **الأثر القانوني:** إذا تعرضت المنظمة للاختراق كون أمنها ضعيفًا، فقد تجري مقاضاتها من قبل الزبائن لكشف معلوماتهم الخاصة، تكون تكلفة التبعات القانونية مكلفة ومرتفعة جدًا في بعض الدول.

3. **الحرمان من الخدمة:** يهدف هجوم رفض الخدمة إلى إغلاق جهاز أو نظام، مما يجعل الوصول إليه غير ممكن للمستخدمين، تُحدد التكلفة من خلال مدى أهمية البنية التحتية لتكنولوجيا المعلومات للأعمال بالنسبة لعملياتها ومقدار الإيرادات التي يخسرونها في مدة زمنية معينة.
4. **العلامة التجارية:** تترك الهجمات الإلكترونية على شركة تجارية سمعة مشوهة لأنها تؤثر بشكل كبير على الطريقة التي يرى بها الناس الشركة، الزبائن الذين كانوا مخلصين لعلامة تجارية أو شركة لعقود من الزمن سوف يتحركون ببطء ويبدأون في إجراء المعاملات مع المنافسين، السبب الأكثر شيوعاً هو خصوصية البيانات وأمانها المهمان للغاية، إذا فشلت الشركة في حماية بيانات زبائنهم، فسوف تفقد ثقتها.



الشكل (3) آثار الهجوم الإلكتروني على المنظمة

المصدر: من إعداد الباحث.

أنواع الأمن السيبراني

سبق وتم التطرق إلى مفهوم الأمن السيبراني والذي يمثل مجموعة من العمليات اللازمة لاتخاذ تدابير أمنية مختلفة، وذلك من أجل حماية الشبكات وأي نوع من البيانات الشخصية من التهديدات الإلكترونية، وفيما يلي أبرز أنواع الأمن السيبراني:

1. **أمن الشبكات Network Security:** هو تقنية تمكن المنظمات من تأمين شبكات الحواسيب من المتسللين والمهاجمين المستهدفين والبرامج الضارة الانتهازية، نظراً لأن الإنترنت به مجموعة متنوعة من الشبكات المرتبطة بمختلف المواقع الإلكترونية، غالباً ما يُلاحظ أن المنظمات أصبحت مستهدفة بالتطفل غير المصرح به، بقصد ضار نظراً لأن العديد من المواقع الإلكترونية تحتوي

على ملفات تعريف ارتباط خاصة بطرف ثالث، يجري من خلالها تتبع أنشطة المستخدمين، في بعض الأحيان قد يكون هذا مفيداً للمنظمات في تنمية أعمالها، ولكن غالباً ما يقع الزبائن فريسة للاحتيال، ومن ثم مواجهة الهجمات الإلكترونية والبرامج الضارة المرتبطة بالشبكة، لذا يتوجب على المنظمات نشر برنامج أمان لمراقبة الشبكة الداخلية والبنية التحتية، ولهذا اقترح الخبراء الاستفادة من تقنية التعلم الآلي التي تقوم بتنبه السلطات في حالة حدوث حركة مرور غير طبيعية، لذا يجب على المنظمات الاستمرار في ترقية أمان شبكاتهما من خلال تنفيذ السياسات التي يمكنها إحباط الهجمات الإلكترونية (Sharif & Mohamed, 2008: 12).

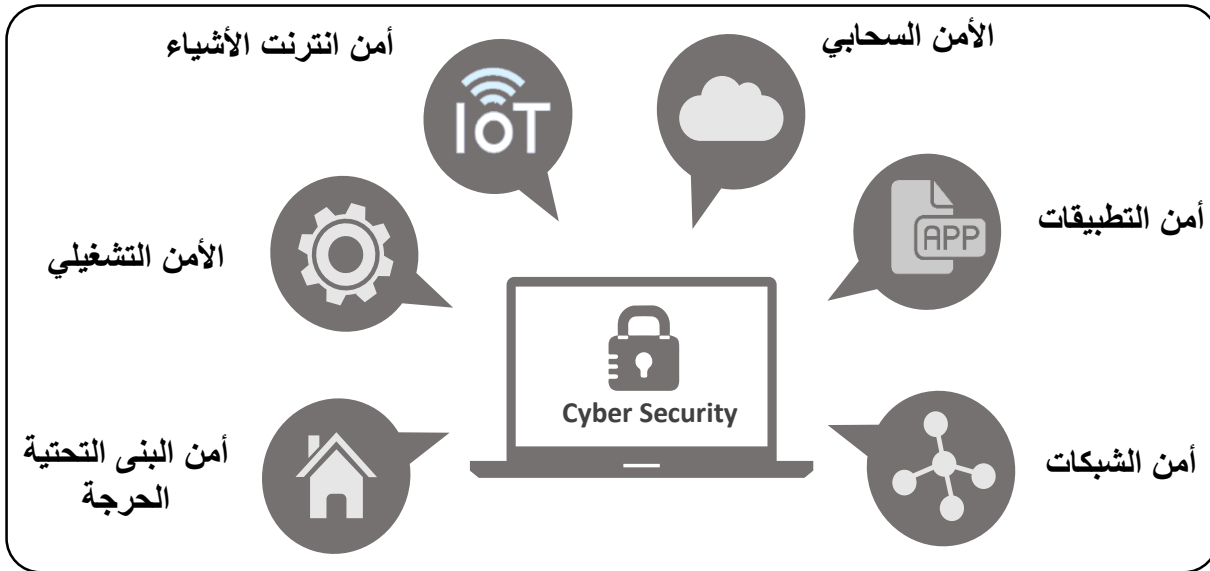
2. أمن التطبيقات Applications security: والذي يسعى إلى إفضال أي نوع من الهجمات المؤثرة على الأمن السيبراني، وذلك بواسطة استخدام العديد من الأجهزة والبرامج، ومن خلال هذا النوع تستطيع الشركات أو المنظمات اكتشاف مجموعة البيانات الحساسة، والتي يجب حمايتها بشكل كبير، وهناك طرق عدة مرتبطة بأمن التطبيقات، وهي (برنامج مضاد للفيروسات، جدران الحماية وعملية التشفير) والتي يتم القيام بها من خلال برامج خاصة (Han & others, 2021: 3197).

3. الأمن السحابي Cloud Security: تميل معظم المنظمات الآن نحو استخدام الذكاء الاصطناعي لتحسين أعمالها، وتعزيز تجربة الزبائن، والعمليات الفعالة، مع وفرة البيانات المتاحة في كل خطوة من خطوات الإعداد التنظيمي، يصبح من الصعب على المنظمات تخزين هذه البيانات في شكل مادي، وكذلك يُلاحظ أن هذه البيانات غالباً ما تكون غير منظمة ومشتقة من مصادر غير معروفة، مما قد يتسبب في تهديد محتمل لشبكة المنظمة، وتقدم بعض الشركات خدمات لزيائنها مثل Amazon Web Services و Microsoft Azure و Google Cloud وهي نظام أساسي للحوسبة السحابية، حيث يمكن للمستخدمين تخزين البيانات ومراقبتها من خلال تطبيقه (Chandra, 2019: 2072).

4. أمن إنترنت الأشياء Internet of Things security: إنَّ إنترنت الأشياء هو الأداة التالية للثورة التكنولوجية، قدر تقرير صادر عن شركة Bain and Company أنّ حجم السوق لإنترنت الأشياء سيتوسع بمقدار كبير جداً وبمساعدة شبكة الأمان الخاصة بها، يوفر إنترنت الأشياء للمستخدم مجموعة متنوعة من الأجهزة المهمة وغير الحيوية مثل أجهزة الاستشعار والطابعات وأجهزة التوجيه Wi-Fi (Oriol, 2020).

5. الأمن التشغيلي Operational Security: يهدف إلى إدارة المخاطر لجميع مجالات الأمن السيبراني الداخلي، وغالبًا ما يقوم باستخدام هذا النوع مجموعة من مسؤولي إدارة المخاطر، وذلك لضمان وجود خطة بديلة إذا ما تعرضت أحد بيانات المستخدمين لأي هجوم كان، كذلك يضم الأمن التشغيلي بيانًا يشمل على توضيح كيفية توعية الموظفين بأفضل الأعمال التي يجب القيام بها، من أجل حماية أمن المعلومات الشخصية والتجارية (الروسان وأبو عليم، 2021).

6. أمن البنية التحتية الحرجة Critical infrastructure security: يجري نشر تقنية الأمن السيبراني للبنية التحتية الحيوية لتأمين الأنظمة التي تحتوي على البنية التحتية الحيوية، وهي الأنظمة التي تعتمد عليها المجتمعات بشكل كبير، وتشمل (شبكة الكهرباء، وتنقية المياه، وإشارات المرور، ومراكز التسوق، والمستشفيات) التي ليست مرتبطة بشكل مباشر، ولكنها يمكن أن تعمل كمنصة من خلالها تحدث البرامج الضارة في النقاط التي تتصل بها هذه الأنظمة.



الشكل (4) أنواع الامن السيبراني

المصدر: من إعداد الباحث.

تهديدات الأمن السيبراني

1. البرامج الضارة Malware

تعد أكثر أشكال التهديد الإلكتروني الأمني انتشارًا وشيوعًا هي البرامج الضارة، إذ وجدت منذ بداية الإنترنت ولا تزال تمثل مشكلة مستمرة، البرامج الضارة هي عندما يقوم جزء غير مرغوب فيه من البرمجة أو البرنامج بتنشيط نفسه على نظام ما، فيتسبب في سلوك غير معتاد، ينتج عنه رفض الوصول إلى البرامج، أو حذف الملفات، أو سرقة المعلومات، أو نشر نفسها على أنظمة أخرى (Hamed, 2020: 2).

2. سرقة كلمة المرور Password Theft

مصادقة كلمة المرور هي الأكثر شيوعًا والمستخدم على نطاق واسع بين جميع طرق المصادقة الأخرى نظرًا لأنها لا تحتاج إلى حمل، سهولة التعلم، فعالة في الاستخدام، سهولة الاسترداد ولكن إلى جانب هذه المزايا، هناك جانب سلبي، فهي معرضة بشكل متزايد للهجمات مثل هجمات القوة الغاشمة أو هجمات القاموس أو غيرها من هجمات اختراق كلمات المرور التي تهدف إلى كسر كلمات مرور المستخدمين (Hussien, 2018: 3).

3. اعتراض حركة المرور Traffic Interception

يُعرف كذلك بـ"التنصت"، يحدث عند اعتراض حركة المرور "استماع" طرف ثالث إلى المعلومات المُرسلة بين المستخدم والمضيف، يختلف نوع المعلومات المسروقة بناءً على حركة المرور، ولكن غالبًا ما يتم استخدامها لتسجيل الدخول أو تسجيل بيانات قيمة (Alyoshin, 2020: 163).

4. هجمات التصيد Phishing Attacks

تُعد عمليات التصيد الاحتيالي طريقة هجوم قديمة وتعتمد على الهندسة الاجتماعية لتحقيق هدفها، المتمثلة بسرقة معلومات المستخدم الحساسة، بعض الأمثلة على هجمات التصيد هي الإعلانات المزيفة والمكالمات الصوتية المزيفة ورسائل البريد الإلكتروني الجماعية والرسائل النصية القصيرة المستلمة من عنوان إلكتروني مزيف، كما تُعاني الخدمات المصرفية من عمليات التصيد الاحتيالي والتزيف، حيث يتلقى الأشخاص رسائل بريد عشوائي أو رسائل بريد إلكتروني مزيفة تحاول الوصول إلى بيانات سرية لارتكاب عمليات احتيال، يمكن للضحايا تلقي رسائل بريد إلكتروني تصيدية تعيد توجيههم إلى صفحة إلكترونية أنشأها الخصم والتي تشبه الموقع الشرعي لمزود خدمة الضحية مثل جامعة أو مؤسسة مالية أو بنك، إلخ (Bojjagani, 2020: 1-2).

5. هجوم رفض الخدمة DdoS

رفض الخدمة هو طريقة هجوم تستهدف فيها الأطراف الخبيثة الخوادم وتحميلها بشكل زائد على حركة المرور، مما يتعذر على الخادم التعامل مع الطلبات الواردة، فيتم إغلاق الموقع الإلكتروني الذي يستضيفه أو يتباطأ في الأداء فيصبح غير قابل للاستخدام (Awan & others, 2021: 2).

6. هجوم البرمجة عبر الموقع Cross Site Scripting Attack

في هذه الحالة تستهدف جهة خارجية موقع إلكتروني ضعيف، وعادةً ما يفتقر إلى التشفير، بمجرد حقن البرمجة الخبيثة على موقع إلكتروني ما، ووصول المستخدم العادي إلى هذا الموقع، يتم تسليم حمولة له إما في نظامه أو متصفحه، مما يتسبب في سلوك غير مرغوب به، الهدف هو إما تعطيل الخدمات أو سرقة معلومات المستخدم (Kadhim, 2020: 1028).

7. هجمات يوم الصفر Zero-Day Exploits

عبارة عن هجمات جديدة لم تكن أنماطها معروفة لبرامج وأجهزة الكشف والحماية إذ تجري هذه الهجمات بعد اكتشاف ثغرة جديدة يمكن استغلالها تسمى "ثغرة يوم الصفر" التي تستهدف نظام أو شبكة أو برنامج، وغالبًا تحدث عند وجود مشكلة أمنية جرى التغاضي عنها (Al-rimy & others, 2018: 83).

8. حقن الـSQL Injection

حقن SQL هو نوع من الهجوم يُمكن المهاجم من الوصول إلى البيانات أو تعديلها عن طريق إدخال رمز لغة الاستعلام المكون من انموذج تسجيل الدخول للمواقع الإلكترونية، قد تسمح ثغرة إدخال SQL للمهاجم بإرسال أوامر مباشرة إلى قاعدة البيانات الأساسية للموقع الإلكتروني، وإزالة الخصوصية والوظائف، وهو في الأساس تلاعب بالبيانات، ويتم تنفيذه على قواعد البيانات المصممة بلغة البرمجة SQL للوصول إلى المعلومات التي ليس من المفترض أن تكون متاحة (Latchoumi & Balamurugan, 2020: 3544).

9. الهندسة الاجتماعية Social Engineering

تهدف إلى التلاعب بالأفراد والمؤسسات لإفشاء بيانات قيمة وحساسة لصالح مجرمي الإنترنت، تتحدى الهندسة الاجتماعية أمان جميع الشبكات بغض النظر عن قوة جدران الحماية وطرق التشفير وأنظمة كشف التسلل وأنظمة برامج مكافحة الفيروسات، من المرجح أن يثق البشر في الآخرين مقارنة بأجهزة الحاسوب أو التقنيات، لذلك فهم الحلقة الأضعف في سلسلة الأمان، تؤثر الأنشطة الضارة التي يتم إجراؤها من خلال التفاعلات البشرية على الشخص نفسيًا لإفشاء معلومات سرية أو

لكسر الإجراءات الأمنية، حالياً تُعد هجمات الهندسة الاجتماعية أكبر التهديدات التي تواجه الأمن السيبراني، يمكن اكتشافها ولكن لا يمكن إيقافها، يستفيد المهندسون الاجتماعيون من الضحايا للحصول على معلومات حساسة، والتي يمكن استخدامها لأغراض محددة أو بيعها (Salahdine & Kaabouch, 2019: 1-2).

10. هجوم MitM

هجوم رجل في الوسط (MITM) هو مصطلح عام عندما يضع المهاجم نفسه ما بين العميل والتطبيق، إما للاستماع خلسة أو لتقليد أحد الأطراف، مما يجعل تبادل البيانات تظهر كما لو أنها عادية، وفي التشفير وأمن الحاسوب الشخصي، يُعد هجوم MITM هجوماً ينتقل فيه المهاجم سرّاً ربما يغير المراسلات بين طرفين يثقان بأنهما يتواصلان بشكل مباشر مع بعضهما (1: 2019, Mallik).

11. هجوم الفدية Ransomware

هو نوع من الهجمات الإلكترونية الضارة والتي تحتجز بيانات الضحية رهينة عن طريق تشفيرها على حاسوب المستخدم لجعلها غير متاحة، ويتم فك تشفير البيانات فقط بعد أن يدفع المستخدم فدية على شكل مبلغ من المال (Khan & others, 2020: 119710).

12. هجوم العملات المشفرة Cryptojacking

عبارة عن نشاط ضار يستلزم الاستخدام غير المصرح به لموارد جهاز الضحية مثل وحدة المعالجة المركزية والذاكرة لتعدين العملة المشفرة، يؤدي ذلك إلى استنزاف عمر البطارية وتقليل أداء النظام (1: 2022, Malik & Anwar).

13. هجمات فيروس طروادة Trojan Virus Attacks

أو ما تسمى بهجمات حصان طروادة، تعني أحصنة طروادة أي خدعة أو حيلة تتسبب في دعوة هدف لعدو يتبين للهدف بأنه حصن أو مكان محمي بشكل آمن، ولكن هو عبارة عن برنامج ضار يخدع المستخدمين لتشغيله عن طيب خاطر (2: 2022, Hu & others).

أبعاد الأمن السيبراني

لغرض تناول ابعاد الامن السيبراني تم الاعتماد في هذا المبحث على مقياس دراسة (نخيلان، 2020) لتحديد ابعاد الامن السيبراني وتتمثل هذه الأبعاد بالآتي:

1. **السرية Confidentiality**: تعني السرية في الأمن السيبراني أن الأشخاص أو الأطراف أو الأنظمة المصرح لهم فقط يمكنهم الوصول إلى بيانات محددة، يمكن أن يُعرف هذا بمبدأ الامتياز

الأقل، إذ يجري منح الحد الأدنى من الأشخاص الضروريين فقط الوصول إلى البيانات (Freyhof, 2022: 10).

2. **الخصوصية Privacy:** وتعني الحرية من التدخل غير المصرح به أو الكشف عن معلومات شخصية حول فرد، وفيما يتعلق بالأمن السيبراني فإن الخصوصية هي وصف لحماية البيانات الشخصية للفرد، التي تُنشر وتتداول من خلال وسائط رقمية كالبريد الإلكتروني، الحسابات البنكية، الصور الشخصية، معلومات عن العمل والمسكن وأي بيانات يتم استخدامها في التفاعل عبر الإنترنت أثناء استخدام الحاسب الآلي أو الهاتف المحمول أو أي من وسائل الاتصال الرقمي بالشبكة العنكبوتية (مكاوي ومحمد، 2022: 6).

3. **التعزيز:** يتضمن تعزيز الأمن السيبراني (Cybersecurity Defense) كل من (الهيئة الوطنية للأمن السيبراني: 2018: 19):

أ. إدارة الأصول: التأكد من أن المنظمة لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة لها.

ب. إدارة هويات الدخول والصلاحيات: ضمان حماية الأمن السيبراني للوصول المنطقي إلى الأصول المعلوماتية والتقنية للمنظمة.

ج. حماية البريد الإلكتروني.

د. إدارة أمن الشبكات: ضمان حماية شبكات المنظمة من المخاطر السيبرانية.

هـ. حماية البيانات والمعلومات: ضمان حماية سلامة بيانات ومعلومات المنظمة.

و. التشفير: ضمان الاستخدام السليم والفعال للتشفير لحماية الأصول المعلوماتية الإلكترونية للمنظمة.

ز. إدارة النسخ الاحتياطية: ضمان عمليات النسخ الاحتياطي لبيانات ومعلومات المنظمة للحماية من الأضرار الناجمة عن المخاطر السيبرانية.

ح. اختبار الاختراق: تقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني في المنظمة.

ط. إدارة سجلات الأحداث ومراقبة الأمن السيبراني: ضمان تجميع وتحليل ومراقبة سجلات أحداث الأمن السيبراني.

ي. الأمن المادي: ضمان حماية الأصول المعلوماتية والتقنية للمنظمة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب.

المبحث الثاني

أداء المنظمة

توطئة

يمثل الأداء قدرات وقابلية المنظمة لتحقيق أهدافها الموضوعية، فالمنظمات في الوقت الراهن تسعى لتحقيق أداء متفوق بما يضمن لها موقع جيد في السوق وحصة سوقية متميزة، سيما في ظل التوجه نحو التنافس المفتوح، لذا يستوجب على المنظمات معرفة وضعها الحالي من أجل تحسينه إذا كان ضعيفاً أما إذا كان جيداً فعليها تطويره باستمرار كون طبيعة المحيط يفرض ذلك.

مفهوم الأداء

إنّ تحديد مفهوم دقيق للأداء يعدّ أمراً صعباً وذلك لوجود الصفات المتغيرة التي يكتسبها الأداء، فتارةً يظهر الأداء على أنه قدرة المنظمة على تخصيص مواردها واستخدامها الأمثل، وتارةً يرتبط بإنتاجية العمال والعنصر البشري، وأخرى يظهر على أنه قرين الإنتاجية وصورتها، ومن هذه المفاهيم:

اللغة العربية الأداء - وزان فعال: اسم مصدر للفعل (أدى) ومصدره التأدية، ومعناه- على ما صرح به بعض أهل اللغة - القضاء، يقال: أدى فلان دينه تأديّةً، أي قضاها (الجواهري، 1407هـ: 2266).

أما اصطلاحاً يستعمل الفقهاء لفظ الأداء تارة في المعنى المتقدم عن أهل اللغة، وأخرى في معنى آخر يختصّ بهم هو الإتيان بالمطلوب في وقته المختص، في مقابل القضاء الذي هو اصطلاح خاصّ بهم، معناه: الإتيان بالفعل المطلوب خارج وقته المختص، لتدارك ما بقي من مصلحة الفعل بعد فوات مصلحة الوقت (سعدي، 1408هـ: 355).

أما في اللغة الانكليزية يرجع أصل كلمة أداء إلى الكلمة (Performance) التي تعني الإنجاز، التنفيذ، ومن ثمّ يقصد بالأداء تنفيذ الأعمال بناءً على هدف أو مجموعة أهداف مع مراعاة النتائج المترتبة على ذلك، وعليه فإن لفظ Performance يعني عموماً ثلاثة معانٍ هي (تعبّر عن حدث، تنفيذ عمل ما، تعبّر عن نتيجة حدث أو فعل ما (Ecosip, 1999: 16)).

ويشير (غانم، 2021: 36) الأداء بأنه سلوك يهدف إلى تحقيق نتيجة وهو ما يقوم به الفرد استجابة لمهمة معينة سواء جرى بها بذاته أم فرضها عليه من الآخرين.

وفي علم الإدارة عرّف الأداء بأنه انعكاس لقدرة الوحدة على القيام بعمل معين وانجازه بالصورة الصحيحة وبالخواصّ المطلوبة وبأقل تكلفة ممكنة وصولاً إلى تحقيق الأهداف المطلوبة بكفاءة وفعالية،

ويساعد في تطوير الوحدة ويدعم استمرارها في بيئة الأعمال المحيطة، على أساس أن الأداء يمثل الناتج النهائي لجميع الأنشطة أو الأعمال التي تقوم بها الوحدة (السعدون، 2017: 50).

مفهوم أداء المنظمة

يُعد مفهوم الأداء مهمًا وجوهريًا بالنسبة للمنظمات ويمثّل القاسم المُشترك لأهتتمام الباحثين في علم الإدارة بشكل خاص، وينصب الأداء المنظمي على مخرجات المنظمة التي تسعى لتحقيقها، وهو مفهوم يعكس كلاً من الأهداف والوسائل اللازمة لتحقيق المخرجات ذات القيمة التي ينتجها النظام على شكل خدمات وسلع نتيجة التفاعل بين الانجاز والسلوك على المستوى التنظيمي للوحدات المكونة لهيكل المنظمة أو على مستوى الموارد البشرية، كما أن أداء المنظمة يعكس الأعمال التي تقوم المنظمة من خلالها بتوظيف الموارد والإمكانات المتاحة لديها والتي يترتب عليها كفاءة وفعالية المنظمة (زلط ومحمود، 2022: 540)، وفي الجدول الآتي بعض التعريفات الخاصة بمفهوم الأداء:

جدول (7) تعريفات أداء المنظمة

ت	المصدر	التعريف
1.	(نبيل، 1998)	المنهجية المنظمة لضمان النشاطات التي خطط لها مسبقاً، فهو الأسلوب الأمثل الذي يساعد على منع وتجنب حدوث المشكلات، وذلك من خلال التشجيع على السلوكيات الجيدة، وكذلك الاستخدام الأمثل لأساليب التحكم.
2.	(محمد، 2018)	الغايات التي ترغب أي منظمة في الوصول إليها بكفاءة وفعالية.
3.	(Bibi & Akhtar, 2020)	أنه تحقيق الأهداف المرجوة والتنفيذ الناجح للخطط والسياسات التعليمية، لذلك فإن مفهومه للأداء المنظمي يتجه إلى الجانب العملي للأهداف والغايات.
4.	(بوزاغو، 2021)	انجاز الأهداف التنظيمية باستخدام الموارد بكفاءة وفعالية إذ تمثل الكفاءة تعظيم النتائج باستخدام أقل الموارد، أما الفعاليات تتعلق بانجاز الأهداف المرغوب فيها.
5.	(Ajis & others, 2022)	أنه مجموع الإنجازات المتعلقة بالأهداف التنظيمية.

المصدر: من اعداد الباحث بالاعتماد على الإديبات.

أهمية أداء المنظمة

يمكن القول أنّ حياة المنظمة أيًا كانت طبيعة النشاط الذي تمارسه، تتوقف على أداء العاملين فيها، فإذا ما أنجزوا أعمالهم ومهامهم على الوجه المطلوب والمخطط له من قبل الإدارة، فإن هذا يقود المنظمة نحو

تحقيق أهدافها كالبقاء، والنمو، والتوسع وإذا كان الأداء دون المستوى المطلوب، فإنه سيشكل عائقًا كبيرًا أمام المنظمة في تحقيق أهدافها، بل يؤدي أحيانًا إلى تصفية المنظمة (سليمان، 2016: 20)، يُنظر إلى أداء المنظمة بشكل عام إلى كيفية أداء كل قسم فيها وكذلك أداء كل موظف داخلها (Salman, 2017: 77-78)، وتتمثل أهمية أداء المنظمة بالآتي (حسن وآخرون، 2021: 77-78):

1. يوفر أداء المنظمة مقياسًا لمدى نجاح المنظمة من خلال سعيها لمواصلة نشاطها بغية تحقيق أهدافها.
2. إن أداء المنظمة يظهر مدى إسهامها في عملية التنمية الاقتصادية والاجتماعية من خلال تحقيق أكبر قدر من الإنتاج بأقل التكاليف والتخلص من عوامل الهدر والضياع في الوقت والجهد والمال، مما يؤدي إلى خفض أسعار المنتجات، ومن ثم تنشيط القدرة الشرائية وزيادة الدخل القومي.
3. يوفر نظام الأداء المنظمي معلومات لمختلف المستويات الإدارية في المنظمة لأغراض التخطيط والرقابة واتخاذ القرارات المستندة على حقائق علمية وموضوعية.
4. يظهر أداء المنظمة التطور الذي حققته في مسيرتها نحو الأفضل أو نحو الأسوأ، وذلك عن طريق نتائج التنفيذ الفعلي للأداء زمنيًا في المنظمة من مدة لأخرى ومكانيًا بالمنظمات المتماثلة.
5. يساعد على إيجاد نوع من المنافسة بين الأقسام والإدارات والمنظمات المختلفة وبدوره يدفع المنظمة لتحسين أدائها.
6. يؤدي إلى الكشف عن العناصر الكفوءة ووضعها في المواقع الأكثر إنتاجية وتحديد العناصر التي تحتاج إلى دعم وتطوير من أجل النهوض بأدائها إلى مستوى الأداء الطموح.
7. يؤدي إلى تحقيق الأهداف المحددة في التخطيط والعمل على إيجاد نظام مرن وفعال للاتصالات والمكافآت والحوافز الشخصية.
8. يوضح أداء المنظمة المركز الإستراتيجي لها ضمن إطار البيئة القطاعية التي تعمل فيها، ومن ثم تحديد الآليات وحالات التغيير المطلوبة لتحسين المركز الإستراتيجي لها.
9. تعكس عملية أداء المنظمة درجة الموائمة والإنسجام بين الأهداف والإستراتيجيات المعتمدة لتنفيذها وعلاقتها بالبيئة التنافسية للمنظمة.
10. الأداء الجيد للمنظمات يسهم في زيادة الناتج المحلي الإجمالي للبلد (Salman, 2017: 11).

قياس أداء المنظمة

يُعرّف قياس الأداء على أنه المراقبة المستمرة لإنجازات برامج المنظمة وتوثيقها، سيما مراقبة وتوثيق جوانب سير التقدم نحو تحقيق غايات موضوعة مسبقًا.

ويمكن تعريف قياس الأداء على أنه "عملية قياس ما حققته المنظمة من انجازات مقارنة بالمستويات المراد تحقيقها أو بالإمكان الحصول عليها، أي معاينة مدى تحقق الأهداف وتنفيذ الخطط وتجسيد الاستراتيجيات المنتهجة وكيفية استخدام الموارد، واكتشاف الانحرافات والاختفاء (فاروق وآخرون، 2017: 69).

لا يمكن أن يكون هناك تطوير دون قياس، فإذا كانت المنظمة لا تعلم أين موقعها الآن من جانب واقع عملياتها لا يمكن أن تعرف مستقبلها ومن ثم لا يمكنها من تحقيق أهدافها الاستراتيجية، ويمكن التعبير عن ذلك من خلال المقولة المشهورة "ما لا يمكن قياسه لا يمكن إدارته" ويمكن إيجاز أهمية قياس الأداء في النقاط التالية (طوبينة، 2013: 18-19):

1. إنَّ عملية قياس الأداء تؤدي إلى تحقيق فوائد كثيرة للمنظمة، حيث أنها توفر مدخلًا واضحًا للتركيز على الخطة الاستراتيجية للبرنامج، فضلًا عن غاياته ومستوى أدائه.
 2. القياس يُمكن من تركيز الاهتمام على ما يجب إنجازه ويحفز المنظمات على توفير الوقت والموارد والطاقات اللازمة لتحقيق الأهداف، كما إنَّ القياس يوفر التغذية العكسية حول مجريات سير التقدم نحو الأهداف، وإذ ما كانت النتائج تختلف عن الأهداف يكون بمقدور المنظمة أن تعمل على تحليل الفجوات الموجودة في الأداء وإجراء التعديلات التي تعيدها إلى مسارها المنشود.
 3. إنَّ قياس الأداء يشجع على التوجه بشكل بناء نحو حل المشكلات إذ إنَّ القياس يوفر بيانات حقيقية ملموسة يمكن الاستناد إليها في اتخاذ قرارات سليمة حول عمليات المنظمة.
 4. القياس يزيد من تأثير المنظمة إذ يتم التعرف من خلاله على المحاور التي تحتاج إلى الاهتمام والتركيز ويجعل من الممكن تحقيق التأثير الإيجابي في تلك المحاور.
 5. إنَّ القياس يوفر آلية معينة لرفع التقارير حول أداء برنامج العمل إلى الإدارة العليا.
- يمكن إضافة عناصر لأهمية قياس أداء المنظمة كما ذكرها (زيادة، 2016: 22):

1. تمكين المنظمة من الاستثمار الأمثل لمواردها.
2. يساعد المنظمة على التحقق من القيام بوظائفها بأفضل كفاءة ممكنة.
3. اكتشاف الانحرافات لكل نشاط من أنشطة المنظمة إذ يساعد ذلك على ممارسة الوظيفة الرقابية واتخاذ الإجراءات التصحيحية لمنع تكرارها.
4. تحديد المراكز الإدارية المسؤولة عن الانحرافات.
5. تحقيق التنسيق بين مختلف نشاطات المنظمة.
6. تحقيق معايير الجودة على أساس المواصفات الموضوعية.

7. ترتبط أهمية القياس ارتباطاً وثيقاً بالتخطيط على كافة المستويات سواء على المستوى الوطني ام على مستوى المنظمة.

ومن الأمور المهمة التي يمكن أن تساعد في معرفة مقياس الأداء الجيد هي (حسن وآخرون، 2021: 94):

1. مستوى جودة العمال.
2. مستوى تحقيق الغايات.
3. مستوى رضا العملاء.
4. تطابق الإجراءات والعمليات مع المعايير والمقاييس الإحصائية الموضوعية.
5. مستوى التحسينات وأين ومتى يجب أن تكون.

هناك وسيلتان لقياس أداء الشركة، أحدهما مالي والآخر أداء غير مالي إلى جانب المؤشرات المالية كتقييم لأداء الشركة في أي صناعة، وتوجد العديد من مقاييس الفاعلية الأخرى الخاصة بالصناعة والتي تعكس نجاح المنظمة، على الرغم من أن كلا النوعين من الأداء يُعدان مؤشرات مهمة للغاية، يجب استخدام كل من المؤشرات المالية وغير المالية لقياس أداء الشركة، يُعرف الأداء المالي "أنه قياس نتائج سياسات وعمليات المنظمة من الناحية النقدية"، ويشمل الربحية ونمو المبيعات وحصص السوق والأداء العام، ويُعرّف الأداء غير المالي بأنه "قياس نتائج السياسات والعمليات التنظيمية من الناحية غير النقدية وغير المالية"، وهي تشمل تحقيق أهداف بدء التشغيل، وتوفير وظيفة آمنة للموظفين، والرضا عن أداء المنظمة (Salman، 2017: 40-41).

أبعاد أداء المنظمة

إنّ لأداء المنظمة العديد من الأبعاد، لكن في هذا المبحث سيجري التطرق إلى بعدي الكفاءة والفاعلية كون أغلب الباحثين يربطون الأداء بمدى بلوغ أهداف المنظمة من جهة ومدى استخدام مواردها المتميزة من جهة ثانية، وبعبارة أخرى يتجسّد الأداء بمستويات الكفاءة والفاعلية للمنظمة (رمول وآخرون، 2013: 38-39).

أولاً: الكفاءة Efficiency

تعدد آراء الباحثين والكتاب في تحديد مفهوم الكفاءة فقد عُرفت الكفاءة بأنها الاستثمار الأمثل لجميع موارد المنظمة أو الشركة المادية والمالية والبشرية المتوفرة لها من البيئة المحيطة مما يمكن المنظمة من إدارة عملياتها بصورة صحيحة للحصول على مخرجات أفضل (جاسم، 2021: 95).

فالكفاءة مفهوم يربط بين المدخلات والمخرجات، كلما كانت المخرجات أكبر من المدخلات يتم الحكم على المنظمة بأنها ذات كفاءة (فاروق وآخرون، 2017: 63)، وتأخذ الكفاءة بالاهتمام النسبة المئوية من الموارد المستخدمة فعلياً مقسومة على الموارد التي كان من المقرر أن تستخدم:

$$\text{الكفاءة} = \frac{\text{الموارد المستخدمة فعلياً}}{\text{الموارد المخطط استخدامها}} \times 100$$

من الواضح أن هذا الموضوع يتعلق بمدخلات العملية وبقياس أداء نظام إدارة العملية، وبالطبع من الممكن استخدام الموارد بكفاءة، بينما تكون العملية غير فاعلة (طويبة، 2013: 22-23).

ثانياً: الفاعلية Effectiveness

يُعد ميدان الفاعلية من المفاهيم الشاملة والواسعة في ريادة الأعمال، لذلك فإن إيجاد تعريف محدد ودقيق ومتفق عليه بين الباحثين والكتاب في هذا المجال يعد أمراً صعباً، إذ عُرفت الفاعلية بأنها درجة تحقيق المنظمة لأهدافها، ولكي تكون المنظمة فاعلة فأنها تحتاج لأهداف واضحة من أجل تحقيقها (عدوان، 2019: 18).

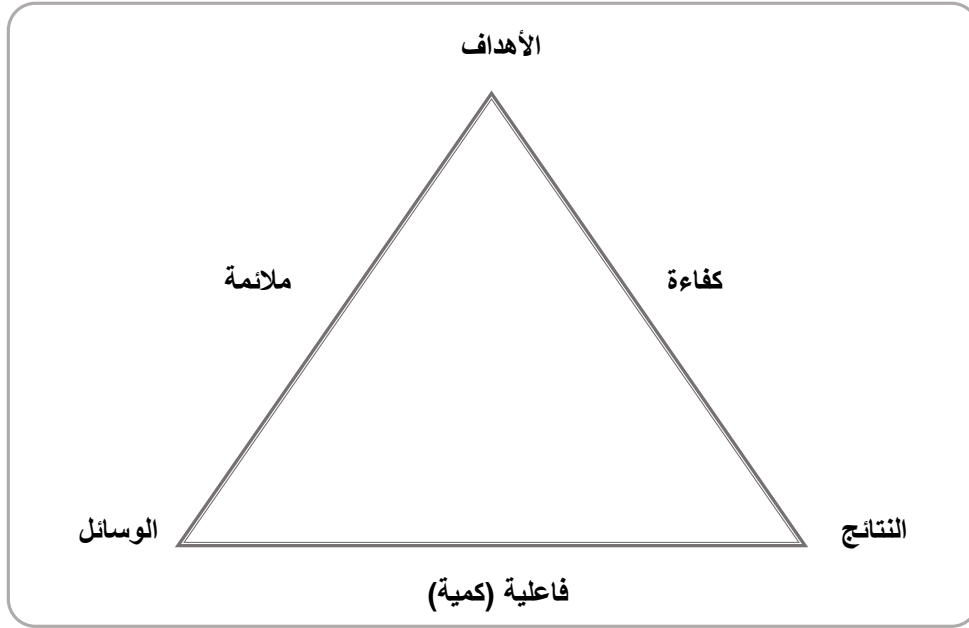
يمكن تعريفها بالنسبة من المخرجات الفعلية مقسومة على المخرجات المتوقعة:

$$\text{الفاعلية} = \frac{\text{المخرجات الفعلية}}{\text{المخرجات المتوقعة}} \times 100$$

مما تقدم يتضح بأن الفاعلية تتعلق بمخرجات العملية وتنفيذ الأهداف وتنفيذ ما تعهد به، قياس الفاعلية يجب أن يعكس ما إذا كانت المنظمة أو مسؤولو العمليات قد نجحوا في تحقيق النتائج المرجوة وتحقيق الصواب يمكن أن تشمل هذه القياسات (طويبة، 2013: 22):

- الجودة: مثل درجة المنتجات أو مستوى الخدمات.
- الكمية: مثل الأطنان، الدفعات عدد غرف النوم المنظفة.
- الالتزام بالوقت: مثل سرعة الاستجابة، وقت التحضير للمنتج، وقت الدورة.
- التكاليف أو السعر: مثل تكلفة الوحدة.

والشكل التالي يوضح العلاقة بين الكفاءة والفاعلية:



الشكل (5) العلاقة بين الفاعلية والكفاءة

المصدر: طويبة، (2013)، تقييم الأداء في ظل بيئة التصنيع الحديثة من خلال التكامل بين المؤشرات المالية وغير المالية بالمسيلة -TINDAL- دراسة حالة مؤسسة الأقمشة والأنسجة الصناعية (Doctoral dissertation، جامعة المسيلة)، ص24، نقلاً عن طاهر محسن منصور الغالبي، أساسيات الأداء وبطاقة التقييم المتوازن، ص48.

الفصل الثالث

الجانب العملي

المبحث الأول: اختبار أداة البحث

المبحث الثاني: التحليل الاحصائي

المبحث الثالث: اختبار فرضيات البحث

الفصل الثالث

الجانب العملي

تمهيد

يشتمل هذا الفصل الاجراءات الميدانية لمتغيرات البحث (تأثير الأمن السيبراني على أداء المنظمة) والمتمثلة بأسلوب جمع البيانات ومعالجتها إحصائيًا وتفسيرها، واجراء اختبار الصدق والثبات للتأكد من مصداقيتها وثبوتيتها، بالإضافة إلى وصف مجتمع وعينة البحث والاساليب الاحصائية التي بموجبها جرى تحليل البيانات واختبار فرضيات البحث.

المبحث الأول

اختبار أداة البحث

توطئة

في هذا المبحث سوف يتم تقييم جودة مقياس البحث لضمان الحصول على نتائج ذات مصداقية وثبوتية عاليتين من خلال اجراء اختبار صدق وثبات الاستبانة.

اختبار صدق وثبات الاستبانة

للتحقق من مصداقية الاستبانة جرى عرض فقراتها (انظر ملحق رقم 1) على مجموعة من الخبراء في اختصاصات مختلفة لغرض التحكيم (انظر ملحق رقم 2)، وتم التعديل على بعض الفقرات بناءً على ملاحظاتهم وتوجيهاتهم لتكون الاستبانة بشكلها النهائي المتضمنة (26) فقرة موزعة على المتغيرين المستقل والتابع بأبعادهما (انظر ملحق رقم 3)، وكذلك تم اجراء الاختبارات التالية:

1. ثبات المقياس

يشير الثبات Reliability إلى درجة الاستقرار أو الاتساق في الدرجات المتحققة على اداة المقياس مع الزمن (عبود، 2017: 225)، بمعنى ان الثبات يعني استقرار (Stability) واتساق (Consistency) المقياس، ومن اشهر المقاييس المستخدمة في قياس ثبات أسئلة الاستبانة هو مقياس (Cronbach's Alpha)، ويشير (Sekrana,2003:311) انه اذا بلغت قيمة الاختبار المذكور أقل من (0.60) فان ذلك يعد مؤشرًا على ضعف ثبات المقياس المُستخدم، في حين يعد ثبات المقياس مقبولًا في حال تعديده نسبة (0.70)، فيما تعد نسبته جيدة إذا بلغت (0.80) فأكثر.

2. صدق المقياس

المقصود بالصدق Validity هو إلى أي درجة يقيس الاختبار ما وضع لقياسه (الضامن، 2015: 113)، بمعنى آخر هل أن المقياس الموضوع يقيس الظاهرة تحت البحث وليس شيئاً آخر (Sekrana,2003:206) والصدق أنواع استخدم الباحث منها صدق المحتوى Content Validity وهو مقياس حكمي Judgmental يعتمد على تحديد الباحث الدقيق لمتغيرات البحث والذي يعتمد على حجم المعلومات التي درسها للموضوع (Cooper & Schindler,2014:257). والباحث استخدم الصدق الظاهري كونه يعد اجراء أولياً لاختيار المقياس وصدق المحتوى (الضامن، 2015: 113)، من خلال إخضاع استمارة الاستبانة للصدق الظاهري وعرضها على مجموعة من الخبراء، والجدول الآتي يبين معاملات الثبات لمتغيرات البحث:

جدول (8) معامل الثبات Cronbach's Alpha لمتغيرات البحث

المتغير	معامل الثبات Cronbach's Alpha
الأمن السيبراني	0.778
أداء المنظمة	0.899

المصدر: من إعداد الباحث بناءً على مخرجات برنامج SPSS.V26

يتضح من الجدول (8) أن قيم معاملات Cronbach's Alpha لمتغيرات البحث هي ضمن الحدود المقبولة احصائياً مما يعني ان المقياس المستخدم لقياس فقرات البحث يتمتع بثبات عالٍ والذي يُمكن الباحث من التعويل عليه لإتخاذ قرار سليم بناءً على النتائج التي سيتم الحصول عليها.

المبحث الثاني التحليل الاحصائي

توطئة

يهدف هذا المبحث إلى عرض وتحليل وتفسير نتائج إجابات أفراد عينة البحث بخصوص الفقرات الواردة في استمارة الاستبانة من خلال استعراض قيم الاوساط الحسابية الموزونة وشدة الإجابة والانحرافات المعيارية ومعاملات الاختلاف لكل فقرة من فقرات متغيرات البحث.

وقد حدد الباحث مستوى الاجابات في ضوء المتوسطات الحسابية من خلال تحديد انتمائها إلى أي فئة، ولأن استمارة البحث تعتمد على مقياس ليكرت الخماسي (أوافق بشدة - لا أوافق بشدة) فإن هنالك خمس فئات تنتمي لها المتوسطات الحسابية، وتحدد الفئة من خلال إيجاد طول المدى (5-1 = 4)، ومن ثم قسمة المدى على عدد الفئات (5) (5 = 4/0.80)، وبعد ذلك يضاف (0.80) إلى الحد الأدنى للمقياس (1) أو يطرح من الحد الأعلى للمقياس (5)، وتكون الفئات مبيّنة في الجدول (9):

جدول (9) الاوساط الحسابية الموزونة ومستويات الاجابة لها

المتوسط الموزون	مستوى الاجابة
من 1 إلى 1.80	منخفض جداً
من 1.81 إلى 2.60	منخفض
من 2.61 إلى 3.40	معتدل
من 3.41 إلى 4.20	مرتفع
من 4.21 إلى 5	مرتفع جداً

Source: Dewberry, Chris,(2004).Statistical Methods for Organizational Research:Theory and practice. First published, Published in the Taylor & Franci, p15.

أولاً: عرض وتحليل وتفسير اجابات أفراد عينة البحث بخصوص الأمن السيبراني سيتم بيان فقرات المتغير الأول من خلال تحليل وشرح الأسئلة المتعلقة به والذي هو الأمن السيبراني وعلى النحو الآتي:

1- السرية

تم قياس البُعد الأول من أبعاد الأمن السيبراني من خلال ستة أسئلة (من 1 إلى 6)، ويبين الجدول (10) أدناه قيم الأوساط الحسابية الموزونة وشدة الإجابة والانحرافات المعيارية ومعاملات الاختلاف المحسوبة سواء كانت على المستوى الجزئي أم الكلي وكالاتي:

جدول (10) الإحصاءات الوصفية لبعد السرية

ت	الفقرة	المتوسط الحسابي \bar{X}	الانحراف المعياري SD	معامل الاختلاف % CV	شدة الإجابة % P
1	لدي كلمة مرور قوية تتكون من رموز وأحرف وأرقام صغيرة وكبيرة.	4.93	0.26	5.35%	98.50%
2	يتم تبادل أرقام المرور السرية للأنظمة الالكترونية بين العاملين في الشركة.	1.63	0.62	38.15%	32.50%
3	لمديري شبكات الشركة القدرة على اعطاء الصلاحيات المختلفة للمستخدمين (قراءة فقط، تعديل، قراءة وكتابة) باستخدام الخصائص التي توفرها الأنظمة المستخدمة في الشركة.	3.65	1.30	35.48%	73.00%
4	تفرض الشركة على موظفيها تبديل كلمات المرور بشكل دوري.	4.73	0.63	13.37%	94.50%
5	توجد تعليمات إدارية صريحة حول حماية النظام من اي تلاعب أو غش.	4.5	0.59	13.15%	90.00%
6	يمتلك العاملون معرفة بتفاصيل عقوبات نشر الوثائق والمعلومات السرية أو افشائها.	4.15	0.85	20.55%	83.00%
	المعدل العام	3.93	0.30	7.70%	78.58%

n=40

المصدر: من إعداد الباحث بناءً على مخرجات برنامج Microsoft Excel 2013.

عند ملاحظة النتائج الواردة في الجدول (10) تبين الآتي:

أ. على المستوى الكلي حقق البُعد وسطاً حسابياً موزوناً بلغ (3.93) بمعنى انه يقع ضمن فئة (مرتفع)، فيما بلغت شدة الإجابة (78.58%)، أما قيمة الانحراف المعياري كانت (0.30)، في حين بلغت نسبة معامل الاختلاف نحو (7.70%)، مما تقدم يتضح ان السرية متوافرة في المنظمة المبحوثة.

ب. أما على المستوى التفصيلي فقد حققت الفقرة (1) أعلى وسط حسابي موزون حيث بلغ (4.93) حيث يقع ضمن فئة (مرتفع جداً) وهذا يدل على قوة تبنى المنظمة لهذه الفقرة، وان قيمة الانحراف المعياري بلغت (0.63)، كما ان شدة الإجابة كانت الأولى من بين الفقرات اذ بلغت (98.50%)، وكانت نسبة معامل الاختلاف جيدة بالنسبة إلى الفقرات الأخرى ويدل على شدة تقارب وانسجام إجابات العينة اذ بلغت (5.35%) وهذا يعنى ان موظفي الشركة لديهم الوعي التام بأهمية كلمات المرور المعقدة، في مقابل ذلك نجد ان الفقرة (2) حققت أقل وسط حسابي موزون قياساً بالفقرات الأخرى إذ بلغ (1.63) بانحراف معياري (0.62)، وبشدة إجابة بلغت (32.50%)، وكانت نسبة معامل الاختلاف (38.15%) نلاحظ ان مستوى الإجابة فيها كان (منخفض جداً)، يتبين أن ادراك عينة مجتمع البحث لها اقل من كل الفقرات الأخرى وهذا يعني ضعفها قياساً بباقي فقرات بُعد السرية، لذا يتطلب تعزيز هذه الفقرة.

2- الخصوصية

تم قياس البُعد الثاني من أبعاد الأمن السيبراني من خلال ستة أسئلة (من 7 إلى 12)، ويبين الجدول (11) أدناه قيم الاوساط الحسابية الموزونة وقيم شدة الإجابة وقيم الانحرافات المعيارية ومعاملات الاختلاف المحسوبة سواء أكانت على المستوى الجزئي أو الكلي وعلى النحو الآتي:

جدول (11) الإحصاءات الوصفية لبعد الخصوصية

ت	الفقرة	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %	شدة الإجابة %
		\bar{X}	SD	CV	P
7	تقوم إدارة الشركة بمراجعة صلاحيات المستخدمين على فترات منتظمة.	4.53	0.50	11.04%	90.50%

41.00%	46.21%	0.95	2.05	8	اواجه اختراقات متكررة على بريدي الالكتروني.
92.50%	10.47%	0.48	4.63	9	تعتمد إدارة الشركة عدة تقنيات مثل: المصادقة والترخيص والتشفير لحماية الأنظمة والبيانات الحساسة.
88.00%	18.88%	0.83	4.4	10	يتم تشغيل وتحديث جدار الحماية باستمرار لمنع المتسللين من الوصول للبيانات الشخصية أو بيانات الشركة.
89.50%	16.56%	0.74	4.48	11	تتبنى الشركة سياسات أمن سيبراني بمعايير عالمية للحد من حالات التجسس والتخريب الرقمي.
89.00%	24.07%	1.07	4.45	12	تقيم الشركة ورش عمل ودورات تدريبية متخصصة للمستفيدين حول طرق حماية وأمن المعلومات.
81.75%	10.43%	0.43	4.09	المعدل العام	

n=40

المصدر: من إعداد الباحث بناءً على مخرجات برنامج Microsoft Excel 2013.

عند تدقيق النتائج الواردة في الجدول (11) تبين الآتي:

أ. على المستوى الكلي حقق البعد وسطاً حسابياً موزوناً بلغ (4.09) بمعنى انه يقع ضمن فئة (مرتفع)، فيما بلغت شدة الإجابة (81.75%)، أما قيمة الانحراف المعياري كانت (0.43)، في حين بلغت نسبة معامل الاختلاف نحو (10.43%)، مما تقدم يتضح ان الخصوصية متوافرة في المنظمة المبحوثة.

ب. أما على المستوى التفصيلي فقد حققت الفقرة (9) أعلى وسط حسابي موزون حيث بلغ (4.63) حيث يقع ضمن فئة (مرتفع جداً) وهذا يدل على قوة تبني المنظمة لهذه الفقرة، وإن قيمة الانحراف المعياري بلغت (0.48)، كما ان شدة الإجابة كانت الأعلى من بين الفقرات الأخرى اذ بلغت (92.50%)، وكانت نسبة معامل الاختلاف جيدة بالنسبة إلى

الفقرات الأخرى ويدل على شدة تقارب وانسجام إجابات العينة إذ بلغت (10.47%) وهذا يعني إن المنظمة تعتمد تقنيات عدة مثل: المصادقة والترخيص والتشفير لحماية الأنظمة والبيانات الحساسة، في مقابل ذلك نجد ان الفقرة (8) حققت أقل وسط حسابي موزون قياساً بالفقرات الأخرى إذ بلغ (2.05) بانحراف معياري (0.95)، وبشدة إجابة بلغت (41.00%)، وكانت نسبة معامل الاختلاف (46.21%) نلاحظ انها تتمتع بمستوى إجابة (منخفض)، إذ كان ادراك عينة مجتمع البحث لها اقل من كل الفقرات الأخرى وهذا يعني ضعفها قياساً بباقي فقرات بُعد الخصوصية، لذا يتطلب تعزيز هذه الفقرة.

3- التعزيز

تم قياس البُعد الثالث من أبعاد الأمن السيبراني بواسطة ستة أسئلة (من 13 إلى 18)، وبيّن الجدول (12) قيم الاوساط الحسابية الموزونة وقيم شدة الإجابة وقيم الانحرافات المعيارية ومعاملات الاختلاف المحسوبة سواء على المستوى الجزئي ام الكلي كما مبين أدناه:

جدول (12) الإحصاءات الوصفية لبعد التعزيز

ت	الفقرة	المتوسط الحسابي \bar{X}	الانحراف المعياري SD	معامل الاختلاف % CV	شدة الإجابة % P
13	تعتمد الشركة وسائل لتحديد الموظفين الذين لديهم صلاحية الوصول إلى موقع معالجة وخرن البيانات.	4.68	0.47	10.02%	93.50%
14	تستخدم برامج مكافحة الفيروسات والمتجسسات المرخصة بشكل دوري في أجهزة الشركة لحمايتها من البرامج الضارة.	4.53	0.50	11.04%	90.50%
15	يتم حماية الأنظمة التشغيلية (Operating Systems OS) باستخدام أجهزة (Hardware) حماية متطورة وبرامجيات (Software) حماية، أو اعتماد آليات من تصميم الشركة ذاتها.	4.1	1.14	27.70%	82.00%

16	توجد آليات تخزين آمنة للوثائق إلى جانب وجود نسخ احتياطية (Backup) لكافة ملفات ومعلومات الشركة في اقراص صلبة أو سحابة خاصة بالشركة.	4.3	0.71	16.61%	86.00%
17	لدى الشركة وسائل لمراقبة البيانات وتحديد المخترق منها وبالتالي يمكن عزلها ومحاولة علاجها.	4.53	0.50	11.04%	90.50%
18	تُحدث إدارة الشركة باستمرار آليات تعزيز حماية شبكتها من خلال مواكبة الاتجاهات والمعايير العالمية المتخصصة بهذا المجال.	4.63	0.62	13.40%	92.50%
المعدل العام		4.46	0.50	11.24%	89.17%

n=40

المصدر: من إعداد الباحث بناءً على مخرجات برنامج Microsoft Excel 2013.

عند تدقيق النتائج الواردة في الجدول (12) تبين الآتي:

أ. على المستوى الكلي حقق البُعد وسطاً حسابياً موزوناً بلغ (4.46) بمعنى انه يقع ضمن فئة (مرتفع جداً)، فيما بلغت شدة الإجابة (89.17%)، أما قيمة الانحراف المعياري كانت (0.50)، في حين بلغت نسبة معامل الاختلاف نحو (11.24%)، مما تقدم يتضح ان التعزيز متوافر في المنظمة المبحوثة.

ب. أما على المستوى التفصيلي فقد حققت الفقرة (13) أعلى وسط حسابي موزون حيث بلغ (4.68) حيث يقع ضمن فئة (مرتفع جداً) وهذا يدل على قوة تبنى المنظمة لهذه الفقرة، وان قيمة الانحراف المعياري بلغت (0.47)، كما ان شدة الإجابة كانت الأعلى من بين الفقرات الأخرى اذ بلغت (93.50%)، وكانت نسبة معامل الاختلاف جيدة بالنسبة إلى الفقرات الأخرى ويدل على شدة تقارب وانسجام إجابات العينة اذ بلغت (10.02%) وهذا يعني ان المنظمة تعتمد وسائل لتحديد الموظفين الذين لديهم صلاحية الوصول إلى موقع معالجة وخرن البيانات، في المقابل نجد ان الفقرة (15) حققت أقل وسط حسابي موزون قياساً بالفقرات الأخرى إذ بلغ (4.1) بانحراف معياري (1.14)، وبشدة إجابة بلغت

(82.00%)، وكانت نسبة معامل الاختلاف (27.70%) نلاحظ انها تتمتع بمستوى إجابة (مرتفع)، ولكن كان ادراك عينة مجتمع البحث لها اقل من كل الفقرات الاخرى وهذا يعني ضعفها قياساً بباقي فقرات بُعد التعزيز، مما يتطلب تعزيز هذه الفقرة.

والجدول (13) يوضح ترتيب ابعاد متغير الأمن السيبراني والبُعد الأكثر أهمية من بين الابعاد الأخرى:

جدول (13) ترتيب ابعاد الأمن السيبراني

ت	البعد	المتوسط الحسابي \bar{X}	الانحراف المعياري SD	معامل الاختلاف % CV	شدة الإجابة % P	ترتيب البعد
1	السرية	3.93	0.30	7.70%	78.58%	1
2	الخصوصية	4.09	0.43	10.43%	81.75%	2
3	التعزيز	4.46	0.50	11.24%	89.17%	3
-	الأمن السيبراني	4.16	0.35	8.37%	83.17%	-

المصدر: من إعداد الباحث بناءً على مخرجات برنامج Microsoft Excel 2013.

يتضح من الجدول رقم (13) ان متغير الأمن السيبراني حقق وسطاً حسابياً موزوناً بلغ (4.16) اذ يقع في فئة (مرتفع) وبانحراف معياري قدره (0.35) ومعامل اختلاف (8.37%) وهذا يدل على توافر هذا المتغير في المنظمة المبحوثة وما يعزز ذلك ان شدة الإجابة كانت (83.17%).

أما بالنسبة للأبعاد فقد نال بُعد السرية المرتبة الاولى ثم جاء بعده بُعد الخصوصية وأخيراً التعزيز.

ثانياً: عرض وتحليل وتفسير اجابات أفراد عينة البحث بخصوص أداء المنظمة

سيتم بحث فقرات هذا المتغير من خلال تحليل وشرح الاسئلة المتعلقة بأبعاد المتغير الثاني وهو أداء المنظمة على النحو الآتي:

1- الكفاءة

تم قياس البُعد الاول من أبعاد أداء المنظمة من خلال أربعة أسئلة (من 1 إلى 4)، إذ يُبين الجدول (14) قيم الأوساط الحسابية الموزونة وشدة الاجابة والانحرافات المعيارية ومعاملات الاختلاف المحسوبة على المستوى الجزئي أو الكلي، كما مبين في الجدول الآتي:

جدول (14) الإحصاءات الوصفية لبعء الكفاءة

ت	الفقرة	المتوسط الحسابي \bar{X}	الأنحراف المعياري SD	معامل الاختلاف % CV	شدة الإجابة % P
1	تسعى الشركة في استثمارها للموارد المتاحة إلى اغناء أعمالها بالمزيد من الخدمات التنافسية.	4.7	0.46	9.75%	94.00%
2	تسعى الشركة إلى تحقيق اهدافها في تعزيز الميزة التنافسية من خلال تطوير عملياتها وخلق منتجات وخدمات خاصة بها قادرة على اضافة مخرجات كفاءة للعمليات الانتاجية نسبة إلى مدخلاتها.	4.53	0.63	13.97%	90.50%
3	تتحقق الخطط الانتاجية الخاصة بعمليات الشركة في تطوير الخدمات الجديدة بصورة كفاءة.	4.38	0.62	14.17%	87.50%
4	تسهم التقنيات المستعملة في تخطيط وتطوير الخدمات الجديدة في زيادة معدلات أرباح الشركة وزيادة معدلات العوائد على الاستثمار وحق الملكية ومعدلات دوران رأس المال.	4.53	0.50	11.04%	90.50%
	المعدل العام	4.53	0.43	9.41%	90.63%

n=40

المصدر: من إعداد الباحث بناءً على مخرجات برنامج Microsoft Excel 2013.

عند تدقيق النتائج الواردة في الجدول رقم (14) تبين ما يلي:

أ. على المستوى الكلي حقق بعء الكفاءة وسطاً حسابياً موزوناً بلغ (4.53) بمعنى أنه يقع

ضمن فئة (مرتفع جداً)، فيما بلغت شدة الإجابة (90.63%)، أما قيمة الأنحراف المعياري

كانت (0.43)، في حين بلغت نسبة معامل الاختلاف نحو (9.41%)، مما تقدم يتضح ان بعد الكفاءة متوافر في المنظمة المبحوثة.

ب. أما على المستوى التفصيلي فقد حققت الفقرة (1) أعلى وسط حسابي موزون حيث بلغ (4.70) حيث يقع ضمن فئة (مرتفع جداً) وهذا يدل على قوة تبنى المنظمة لهذه الفقرة، وإن قيمة الانحراف المعياري بلغت (0.46)، كما ان شدة الإجابة كانت الأعلى من بين الفقرات الأخرى اذ بلغت (94.00%)، وكانت نسبة معامل الاختلاف جيدة بالنسبة إلى الفقرات الأخرى ويدل على شدة تقارب وانسجام إجابات العينة اذ بلغت (9.75%) وهذا يعنى ان المنظمة تسعى في استثمارها للموارد المتاحة إلى اغناء أعمالها بالمزيد من الخدمات التنافسية، في المقابل نجد ان الفقرة (3) حققت أقل وسط حسابي موزون قياساً بالفقرات الأخرى إذ بلغ (4.38) بانحراف معياري (0.62)، وبشدة إجابة بلغت (87.50%)، وكانت نسبة معامل الاختلاف (14.17%) نلاحظ انها تتمتع بمستوى إجابة (مرتفع جداً)، ولكن كان ادراك عينة مجتمع البحث لها اقل قياساً بباقي فقرات بُعد الكفاءة، مما يتطلب تعزيز هذه الفقرة.

2- الفاعلية

تم قياس البعد الثاني من أبعاد أداء المنظمة بواسطة أربعة أسئلة (من 5 إلى 8)، ويبين الجدول (15) قيم الأوساط الحسابية الموزونة وقيم شدة الإجابة وقيم الانحرافات المعيارية ومعاملات الاختلاف المحسوبة سواء على المستوى الجزئي ام الكلي وكالاتي:

جدول (15) الإحصاءات الوصفية لبعد الفاعلية

ت	الفقرة	المتوسط الحسابي	الانحراف المعياري	معامل الاختلاف %	شدة الإجابة %
		\bar{X}	SD	CV	P
5	تمتلك الشركة القدرة على تطوير خدمات جديدة أكثر في سبيل تحقيق أهدافها وتوجهاتها.	4.50	0.50	11.11%	90.00%
6	تسعى الشركة إلى تحقيق رضا جميع الاطراف التي لها علاقة بتقديم الخدمات من أجل تحقيق	4.20	0.98	23.33%	84.00%

				الفاعلية في عمليات تخطيط وتطوير الخدمات الجديدة.
92.00%	13.58%	0.62	4.60	7 تعمل كل الوحدات أو النظم الفرعية باتجاه واحد في سبيل تحقيق أهداف الشركة.
91.50%	12.83%	0.59	4.58	8 تسهم التقنية المستخدمة لتخطيط وتطوير خدمات جديدة تدعم زيادة القيمة الاجمالية للشركة.
89.38%	11.34%	0.51	4.47	المعدل العام

n=40

المصدر: من إعداد الباحث بناءً على مخرجات برنامج Microsoft Excel 2013.

عند تدقيق النتائج الواردة في الجدول رقم (15) تبين ما يلي:

أ. على المستوى الكلي حقق بعد الفاعلية وسطاً حسابياً موزوناً بلغ (4.47) بمعنى أنه يقع ضمن فئة (مرتفع جداً)، فيما بلغت شدة الإجابة (89.38%)، أما قيمة الانحراف المعياري كانت (0.51)، في حين بلغت نسبة معامل الاختلاف نحو (11.34%)، مما تقدم يتضح أن بعد الفاعلية متوافر في المنظمة المبحوثة.

ب. أما على المستوى التفصيلي فقد حققت الفقرة (7) أعلى وسط حسابي موزون حيث بلغ (4.60) حيث يقع ضمن فئة (مرتفع جداً) وهذا يدل على قوة تبنى المنظمة لهذه الفقرة، وإن قيمة الانحراف المعياري بلغت (0.62)، كما ان شدة الإجابة كانت الأعلى من بين الفقرات الأخرى إذ بلغت (92.00%)، وكانت نسبة معامل الاختلاف جيدة بالنسبة إلى الفقرات الأخرى مما يدل على شدة تقارب وانسجام إجابات العينة إذ بلغت (13.58%) وهذا يعنى عمل كل الوحدات أو النظم الفرعية في المنظمة باتجاه واحد في سبيل تحقيق أهدافها، في المقابل نجد ان الفقرة (6) حققت أقل وسط حسابي موزون قياساً بالفقرات الأخرى إذ بلغ (4.20) بانحراف معياري (0.98)، وبشدة إجابة بلغت (84.00%)، وكانت نسبة معامل الاختلاف (23.33%) نلاحظ انها تتمتع بمستوى إجابة (مرتفع)، ولكن كان ادراك عينة مجتمع البحث لها اقل قياساً بباقي فقرات بُعد الفاعلية الأخرى، لذا يتطلب تعزيز هذه الفقرة.

إنّ النتائج المذكورة تدعم النتائج المتوصل إليها على مستوى الابعاد الفرعية من ادراك عينة البحث لأبعاد متغير أداء المنظمة في الشركة المبحوثة، والجدول رقم (16) يوضح ترتيب أبعاد متغير أداء المنظمة والبُعد الأكثر أهمية من بين الابعاد الأخرى:

جدول (16) ترتيب ابعاد أداء المنظمة

ت	البعد	المتوسط الحسابي \bar{X}	الانحراف المعياري SD	معامل الاختلاف % CV	شدة الإجابة % P	ترتيب البعد
1	الكفاءة	4.53	0.43	9.41%	90.63%	1
2	الفاعلية	4.47	0.51	11.34%	89.38%	2
-	أداء المنظمة	4.50	0.44	9.92%	90.00%	-

المصدر: من إعداد الباحث بناءً على مخرجات برنامج Microsoft Excel 2013.

يتضح لنا من الجدول رقم (16) ان متغير أداء المنظمة حقق وسطاً حسابياً موزوناً (4.50) اذ يقع ضمن فئة (مرتفع جداً) وبانحراف معياري (0.44) ومعامل اختلاف (9.92%) والذي يدل على توافر هذا المتغير في المنظمة المبحوثة والذي يعزز ذلك شدة الإجابة التي بلغت (90.00%)، اما بالنسبة للأبعاد فقد نال بُعد الكفاءة المرتبة الاولى وجاء بعده بُعد الفاعلية.

المبحث الثالث

اختبار فرضيات البحث

توطئة

في هذا المبحث سوف يتم اختبار علاقات الارتباط والتأثير بين متغيرات البحث، إذ سيتم اختبار علاقات الارتباط والتأثير على مستوى الفرضيات الفرعية المنبثقة من الفرضيات الرئيسية وكذلك اختبار علاقات الارتباط والتأثير على المستوى الكلي عن طريق استخدام معامل الارتباط (Pearson) ومعامل الانحدار الخطي البسيط.

أولاً: اختبار الفرضية الرئيسية الأولى H0

هذه الفرضية متعلقة بالارتباط بين الأمن السيبراني وأداء المنظمة والتي تنص (لا توجد علاقة ارتباط ذات دلالة معنوية بين الأمن السيبراني بأبعاده وأداء المنظمة بأبعاده)، ولقد تفرع عنها ثلاث فرضيات فرعية كما مبين أدناه:

1. لا توجد علاقة ارتباط ذات دلالة معنوية بين السرية وأداء المنظمة بأبعاده.

2. لا توجد علاقة ارتباط ذات دلالة معنوية بين الخصوصية وأداء المنظمة بأبعاده.

3. لا توجد علاقة ارتباط ذات دلالة معنوية بين التعزيز وأداء المنظمة بأبعاده.

يظهر الجدول (17) مصفوفة معاملات الارتباط البسيط (Pearson) بين المتغيرات وأبعاده، وقبل الدخول في اختبار هذه الفرضية فإن الجدول (17) يشير كذلك إلى حجم عينة البحث البالغة (40) ونوع الاختبار (2-tailed) ومختصر (Sig.) في الجدول يُشير إلى اختبار معنوية معامل الارتباط، فإذا ظهر وجود علامة (*) على معامل الارتباط هذا يعني أن الارتباط معنوي عند مستوى (5%)، أما في حال وجود علامة (**) على معامل الارتباط فإن ذلك يعني أن الارتباط معنوي عند مستوى (1%)، ويجري الحكم على مقدار قوة معامل الارتباط في ضوء قاعدة (Cohen, 1977:79-81)، وكالاتي:

- علاقة الارتباط منخفضة: إذا كانت قيمة معامل الارتباط يتراوح بين (0.10 إلى 0.29).
- علاقة الارتباط متوسطة: إذا كانت قيمة معامل الارتباط يتراوح بين (0.30 إلى 0.49).
- علاقة الارتباط قوية: إذا كانت قيمة معامل الارتباط يتراوح بين (0.5 إلى 1).

جدول (17) اختبار الفرضية الرئيسية الاولى (فرضية الارتباط)

-	-	السرية	الخصوصية	التعزيز	الأمن السيبراني
أداء المنظمة	Pearson Correlation	.652**	.807**	.757**	.882**
	Sig. (2-tailed)	.000	.000	.000	.000
	n	40	40	40	40

المصدر: من اعداد الباحث بالاعتماد على مخرجات برنامج SPSS:V26

يظهر جدول رقم (17) مصفوفة الارتباط لإختبار الفرضية الرئيسية الاولى وما تفرع عنها من فرضيات بأن هناك علاقات ارتباط موجبة قوية (لأن قيمتها أكبر 0.50) وذات دلالة معنوية عند مستوى (1%) بين متغير أداء المنظمة والأمن السيبراني، إذ بلغت قيم معامل الارتباط بين الأمن السيبراني وأداء المنظمة (0.882) عند مستوى دلالة (1%) وتعد علاقة قوية في ضوء قاعدة (Cohen).

أما على مستوى الابعاد كانت أقوى علاقة ارتباط بين الخصوصية وأداء المنظمة، إذ بلغت قيمة علاقة الارتباط بينهما (0.807) عند مستوى دلالة (1%) وتعد علاقة طردية قوية في ضوء قاعدة (Cohen) بينما كانت أضعف علاقة ارتباط بين السرية وأداء المنظمة، إذ بلغت قيمة علاقة الارتباط بينهما (0.652) وتعد علاقة ارتباط قوية في ضوء قاعدة (Cohen).

وتدل النتائج المستحصل عليها من الجدول رقم (17) عدم قبول فرضية عدم الوجود بالنسبة للفرضية الرئيسية الأولى وفرضياتها الفرعية، والتي تنص على أنه (لا توجد علاقة ارتباط ذات دلالة معنوية بين الامن السيبراني بأبعاده وأداء المنظمة بأبعاده). والقبول بفرضية الوجود البديلة بالنسبة للفرضية الرئيسية الاولى وفرضياتها الفرعية، والتي تنص على (توجد علاقة ارتباط ذات دلالة معنوية بين الامن السيبراني بأبعاده وأداء المنظمة بأبعاده).

ثانياً: اختبار الفرضية الرئيسية الثانية H0

هذه الفرضية متعلقة بتأثير الأمن السيبراني على أداء المنظمة والتي تنص (لا توجد علاقة تأثير ذات دلالة معنوية لأبعاد الامن السيبراني في أداء المنظمة) مقابل الفرضية البديلة H1: (توجد علاقة تأثير ذات دلالة معنوية لأبعاد الامن السيبراني في أداء المنظمة)، ولقد تفرعت عن الفرضية الرئيسية أعلاه ثلاث فرضيات كالاتي:

- لا توجد علاقة تأثير ذات دلالة معنوية بين السرية وأداء المنظمة.
- لا توجد علاقة تأثير ذات دلالة معنوية بين الخصوصية وأداء المنظمة.
- لا توجد علاقة تأثير ذات دلالة معنوية بين التعزيز وأداء المنظمة.

جدول (18) تقدير علاقة الانحدار الخطي البسيط بين الأمن السيبراني وأداء المنظمة

أداء المنظمة						المتغير التابع
F	F	T	T	R ²	β	المتغير المستقل
الجدولية 1%		الجدولية 1%				
	133.1		11.54	0.77	1.13	الأمن السيبراني
	28.09		5.30	0.43	0.96	السرية
7.35	70.99	2.426	8.44	0.65	0.85	الخصوصية
	50.98		7.14	0.57	0.67	التعزيز

المصدر: من اعداد الباحث بالاعتماد على مخرجات برنامج SPSS:V26

يتضح من نتائج الجدول رقم (18) أن معامل انحدار متغير الأمن السيبراني على أداء المنظمة بلغ (1.13) وهذا يعني انه اذا تغير الأمن السيبراني بمقدار وحدة واحدة فإن أداء المنظمة يزداد بمقدار (113%)، علماً ان التأثير معنوياً وذلك لأن قيمة (T) المحتسبة والبالغة (11.54) أكبر من نظيرتها الجدولية البالغة (2.426) عند مستوى معنوية (1%).

كذلك يتبين أن الأمن السيبراني يفسر ما نسبته (77%) من التغيرات الحاصلة في أداء المنظمة وأما النسبة المتبقية والبالغة (23%) تعود إلى متغيرات أخرى خارج انموذج البحث الحالي، علماً أن الانموذج المقدر معنوي اجمالاً وذلك لأن قيمة (F) المحتسبة (133.1) أكبر من نظيرتها الجدولية والبالغة (7.35) عند مستوى معنوية (1%).

وعليه بناءً على ما تقدم يتم قبول فرضية الوجود البديلة والتي تنص (توجد علاقة تأثير ذات دلالة معنوية لأبعاد الامن السيبراني في أداء المنظمة).

عند الرجوع إلى الجدول (18) ولفرض إثبات صحة الفرضيات الفرعية المُنبثقة عن الفرضية الرئيسية

الثانية اتضح الآتي:

الفرضية الفرعية الأولى: لا توجد علاقة تأثير ذات دلالة معنوية بين السرية وأداء المنظمة.

يتبين من الجدول رقم (18) ما يلي:

- أ. بلغ معامل الانحدار (0.96) وهذا يعني اذا تغير بعد السرية بمقدار وحدة واحدة فان متغير أداء المنظمة سيزداد بمقدار (96%)، علمًا ان التأثير كان معنويًا وذلك لان قيمة (T) المحتسبة والبالغة (5.30) أعلى من مثيلتها الجدولية عند مستوى معنوية (1%) والبالغة (2.426).
- ب. بلغت قيمة معامل تحديد (R^2) حوالي (0.43) وهذا يعني ان البُعد يفسر ما نسبته (43%) من التغيرات التي تطرأ على أداء المنظمة، أما النسبة المتبقية والبالغة (57%) فتعود لعوامل أخرى غير موجودة في الإنموذج الحالي.
- ج. نجد أن قيمة (F) المحتسبة والبالغة (28.09) أعلى من مثيلتها الجدولية والبالغة (7.35) عند مستوى معنوية (1%) عليه نلاحظ أن الأنموذج المُقدر معنوي إجمالاً.
- ومن هنا يستدل الباحث من تحليل نتائج الجدول (18) على قبول فرضية الوجود البديلة التي تنص (توجد علاقة تأثير ذات دلالة معنوية بين السرية وأداء المنظمة).

الفرضية الفرعية الثانية: لا توجد علاقة تأثير ذات دلالة معنوية بين الخصوصية وأداء المنظمة.

يتبين من الجدول رقم (18) ما يلي:

- أ. بلغ معامل الانحدار (0.85) وهذا يعني إذا تغير بعد الخصوصية بمقدار وحدة واحدة فان متغير أداء المنظمة سيزداد بمقدار (85%)، علمًا أن التأثير كان معنويًا وذلك لأن قيمة (T) المُحتسبة والبالغة (8.44) أعلى من مثيلتها الجدولية عند مستوى معنوية (1%) والبالغة (2.426).
- ب. بلغت قيمة معامل تحديد (R^2) حوالي (0.65) وهذا يعني أن البُعد يُفسر ما نسبته (65%) من التغيرات التي تطرأ على أداء المنظمة، أما النسبة المتبقية والبالغة (35%) فتعود لعوامل أخرى غير موجودة في الإنموذج الحالي.
- ج. نجد أن قيمة (F) المحتسبة والبالغة (70.99) أعلى من مثيلتها الجدولية والبالغة (7.35) عند مستوى معنوية (1%) عليه نلاحظ إن الأنموذج المُقدر معنوي إجمالاً.
- يستدل الباحث من تحليل نتائج الجدول (18) على قبول فرضية الوجود البديلة التي تنص (توجد علاقة تأثير ذات دلالة معنوية بين الخصوصية وأداء المنظمة).

الفرضية الفرعية الثالثة: لا توجد علاقة تأثير ذات دلالة معنوية بين التعزيز وأداء المنظمة.

يتبين من الجدول رقم (18) ما يأتي:

أ. بلغ معامل الإنحدار (0.67) وهذا يعني إذا تغير بعد الخصوصية بمقدار وحدة واحدة فإن متغير أداء المنظمة سيزداد بمقدار (67%)، علماً أن التأثير كان معنوياً وذلك لأن قيمة (T) المُحتسبة والبالغة (7.14) أعلى من مثيلتها الجدولية عند مستوى معنوية (1%) والبالغة (2.426).

ب. بلغت قيمة معامل التحديد (R^2) حوالي (0.57) وهذا يعني أن بعد التعزيز يُفسّر ما نسبته (57%) من التغيرات التي تطرأ على أداء المنظمة، أما النسبة المتبقية والبالغة (43%) فتعود لعوامل أخرى غير موجودة في الإنموذج الحالي.

ج. نجد أن قيمة (F) المُحتسبة والبالغة (50.98) أعلى من مثيلتها الجدولية والبالغة (7.35) عند مستوى معنوية (1%) عليه نلاحظ إن الأنموذج المُقدّر معنوي إجمالاً.

يستدل الباحث من تحليل نتائج الجدول (18) على قبول فرضية الوجود البديلة التي تنص (توجد علاقة تأثير ذات دلالة معنوية بين التعزيز وأداء المنظمة).

الفصل الرابع

الاستنتاجات والتوصيات

المبحث الأول: الاستنتاجات

المبحث الثاني: التوصيات

المبحث الأول الاستنتاجات

المبحث يحوي أهم الاستنتاجات التي توصل إليها الباحث اعتماداً على التحليل الإحصائي لبيانات الاستبانة وهي:

1. ترتبط أبعاد الأمن السيبراني التي اعتمدت (السرية، الخصوصية، والتعزيز) مع أداء المنظمة على وفق الترتيب التالي من حيث البعد الأكثر أهمية (السرية، الخصوصية ثم التعزيز).
2. تبين ان الشركة عينة البحث تتبنى الأمن السيبراني من خلال اهتمامها بـ(السرية، الخصوصية، والتعزيز) في أعمالها.
3. تهتم الشركة عينة البحث بتحسين مستويات الأداء لديها وكان هذا واضحاً بالنظر إلى النتائج الخاصة بأبعاد أداء المنظمة (الكفاءة والفاعلية).
4. وجود علاقة ارتباط ذات دلالة معنوية بين الأمن السيبراني بأبعاده واداء المنظمة.
5. وجود علاقة تأثير ذات دلالة معنوية بين الأمن السيبراني بأبعاده وأداء المنظمة وان الأمن السيبراني يفسر نسبة محددة من التغيرات الحاصلة على أداء المنظمة.
6. الشركة عينة البحث تبنت السرية في اعمالها وخصوصاً اعتمادها وسائل لجعل الموظفين يمتلكون كلمات مرور قوية تتكون من رموز واحرف وارقام صغيرة وكبيرة.
7. تبين ان الشركة عينة البحث لديها اهتمام عالٍ بالخصوصية من خلال اعتماد العمل بعدة تقنيات مثل: المصادقة والترخيص والتشفير لحماية الأنظمة والبيانات الحساسة مما ينعكس ايجاباً على أداء المنظمة.

المبحث الثاني

التوصيات

أولاً: توصيات تتعلق بالبحث الحالي

وفقاً للنتائج التي توصل إليها الباحث من خلال الإطار النظري للبحث وواقع التحليل الاحصائي للبيانات تم الخروج بالتوصيات الآتية:

1. توصيات تتعلق بالأمن السيبراني:

- أ. الأهتمام من قبل المنظمات بأبعاد الأمن السيبراني التي اعتمدت في هذا البحث (السرية، الخصوصية، والتعزيز) كونها مرتبطة وتؤثر في أداء المنظمة.
- ب. اهتمام إدارة المنظمة المبحوثة بالخصوصية من خلال حث موظفيها على اتخاذ الحلول السريعة في حال مواجهة أي اختراق على البريد الإلكتروني.
- ج. التعزيز في حماية الانظمة التشغيلية باستخدام أجهزة حماية متطورة وبرامجيات حماية، أو اعتماد آليات من تصميم الشركة ذاتها.

2. توصيات تتعلق بأداء المنظمة:

- أ. الأهتمام بصورة أكثر بالخطط الانتاجية الخاصة بعمليات المنظمة لما لها دور في تطوير الخدمات الجديدة وكونها تؤثر بصورة إيجابية على كفاءة المنظمة.
- ب. السعي بصورة أكثر إلى تحقيق رضا جميع الاطراف التي لها علاقة بتقديم الخدمات من أجل تحقيق الفاعلية في عمليات تخطيط وتطوير الخدمات الجديدة للمنظمة.

ثانياً: توصيات تتعلق بالدراسات المستقبلية

ينصح الباحث باجراء المزيد من الابحاث والدراسات حول موضوع الأمن السيبراني وتأثيره على أداء المنظمة في شركات ومنظمات أخرى وذلك نظراً لقلّة الدراسات التي تطرقت للموضوع.

الْمُصَلِّينَ وَالْمُتَّقِينَ

المصادر والمراجع العربية

القران الكريم

أولاً: الكتب

1. أبو نصر إسماعيل بن حماد الجوهري الفارابي، الصحاح تاج اللغة وصحاح العربية، الجزء السادس، بيروت، دار العلم للملايين، 1407هـ.
2. أحمد سيد مصطفى، إدارة البشر – الأصول والمهارات، القاهرة: دن، 2002م.
3. الضامن ومنذر عبد الحميد. "اساسيات البحث العلمي"، الطبعة الثالثة، 2015م.
4. الهيئة الوطنية للأمن السيبراني، الضوابط الأساسية للأمن السيبراني، 2018م.
5. شريف وسامي محمد، "أمن الشبكات"، 2008م.
6. سالم محمد عبود، الاتجاهات الحديثة في اصول البحث العلمي، الطبعة الرابعة، 2017م.
7. سعدي أبو حبيب، القاموس الفقهي لغة واصطلاحًا، دمشق، دار الفكر، 1408هـ.
8. عبد العزيز مخيمر وآخرون، قياس الأداء المؤسسي للأجهزة الحكومية، القاهرة: منشورات المنظمة العربية للتنمية، 2008م.
9. فاطمة بدر ومعاذ الصباغ، نظرية المنظمة، الإجازة في العلوم الإدارية، من منشورات الجامعة الافتراضية السورية، الجمهورية العربية السورية، 2020م.
10. محمد سعيد سلطان، السلوك التنظيمي، دار الجامعة الجديدة، الإسكندرية، مصر، 2003م.
11. مصطفى محمد، الرضا الوظيفي وأثره على تطوير الأداء، المملكة الأردنية الهاشمية، عمان، دار أبن النفيس للنشر والتوزيع، 2018م.
12. نبيل مرس خليل، الميزة التنافسية في مجال الأعمال، مصر: مركز الإسكندرية للكتاب، 1998م.

ثانياً: البحوث والرسائل والأطاريح

1. بوزاغو. أثر النظام المعلوماتي المالي على أداء المؤسسة - دراسة حالة لواقع النظام المعلوماتي المالي في المؤسسة الجزائرية. Diss. 2021.
2. حسن، أثر إعادة هندسة العمليات الإدارية في الأداء المؤسسي. Diss. جامعة ام درمان الاسلامية، 2021.
3. رمول، "دور الإستثمار في الموارد البشرية في تحسين أداء المؤسسات." (2013).

4. سارة بنت بندر نخيلان، دور الأمن السيبراني في تحقيق جودة الخدمات الإلكترونية بعامادة تقنية المعلومات بجامعة الملك عبد العزيز "دراسة ميدانية"، السعودية: جامعة الملك عبد العزيز، 2020م.
5. طويبة. تقييم الأداء في ظل بيئة التصنيع الحديثة من خلال التكامل بين المؤشرات المالية وغير المالية بالمسيلة-TINDAL- دراسة حالة مؤسسة الأقمشة والأنسجة الصناعية. Diss. جامعة المسيلة، 2013.
6. فاروق، "دور إستراتيجية إدارة الموارد البشرية في تحسين الأداء في المؤسسة." (2017).
7. قاسم كاصد غانم، تأثير جودة التدقيق الداخلي لنظام إدارة الجودة في الأداء التنظيمي، دراسة حالة في شركة مصافي الوسط، بحث لنيل شهادة الدبلوم العالي في إدارة الجودة، جامعة كربلاء - كلية الإدارة والاقتصاد، 2021م.
8. ماهر زيادة، مدى فاعلية استخدام بطاقة الأداء المتوازن لتقييم الأداء الاستراتيجي في المصارف الإسلامية، دراسة ميدانية، لنيل درجة الماجستير في علوم الإدارة - مالية ومصارف، الجمهورية العربية السورية، 2016.
9. محمد سميح جمعه عدوان. فاعلية نظم المعلومات الإدارية ودورها في تحسين إدارة الأزمات: دراسة تطبيقية على وزارتي التنمية الاجتماعية والعمل بقطاع غزة. Diss. 2019.
10. مريم عثمانى. "تطبيق الإدارة الإلكترونية في مجال الخدمات المصرفية بين ضرورة الانفتاح ومخاطر النجاح." (2019).
11. مصطفى سلمان منسي، تأثير الحكومة الإلكترونية في أداء المنظمات: دراسة تحليلية لآراء عينة من ضباط وموظفي مديرية المرور العامة/ مديريةية تسجيل المركبات وإجازات السياقة، لنيل شهادة الدبلوم العالي (المعادل للماجستير) في التخطيط الاستراتيجي الأمني، مكتبة الدراسات العليا - كلية الإدارة والاقتصاد - جامعة كربلاء، 2022.
12. هدى مؤيد حاتم السعدون، استخدام بطاقة الأداء المتوازن في تقويم الأداء الاستراتيجي في جامعة القادسية رسالة ماجستير، كلية الإدارة والاقتصاد، جامعة القادسية، 2017.

ثالثاً: المجالات العلمية

1. أمنة محمد منصور. "تأثير الامن السيبراني على الرقابة الداخلية وانعكاسها على الوحدة الاقتصادية- دراسة استطلاعية لآراء عينة من المدققين والمحاسبين في وزارة التعليم العالي والبحث العلمي." Journal of Administration and Economics 127 (2021): 223-238.

2. حسن عماد مكاوي ومحمد. "الخصوصية الرقمية في القانون الدولي والمواثيق الدولية." مجلة البحوث والدراسات الإعلامية 20.20 (2022): 1-74.
3. زلط، محمد على محمود ومحمد على محمود. "أثر التسويق الأخضر على تحسين الأداء المؤسسي في المنظمات." التجارة والتمويل 42.3 (2022): 530-590.
4. صبا طالب وهاب الموسوي. "دور استراتيجية التسويق في تحسين الأداء المنظمي للمستشفيات الأهلية." The islamic college university journal 47 (2018).
5. عيسى عوض سليمان، دينا. "اثر كفاءة عملية تخطيط الموارد البشرية علي الاداء التنظيمي." المجلة العلمية للدراسات التجارية والبيئية 7. ملحق العدد الرابع (2016): 827-855.
6. ماجد جودة جاسم. "قياس الكفاءة التشغيلية وفاعلية تسليم الخدمة إلى الزبائن بأستخدام تقنية DEA دراسة مقارنة لشركات الاتصالات العاملة في العراق." Journal of Administration and Economics 127 (2021): 92-103.
7. مجدي محمد السيد. "الأمن السيبراني وعلاقته بالمضمون الإعلامي في ظل رؤية مصر 2030." المجلة العربية لبحوث الاعلام والاتصال 2021.35 (2021): 484-514.

رابعًا: المقالات

1. رؤى حمود، مجموعة ريناد لتقنية المعلومات، 6 مزايا خفية يقدمها الامتثال لمعايير الأمن السيبراني لمنظمتك، 2022، تم زيارته بتاريخ 2023/1/3
[الامتثال-لمعايير-الأمن-السيبراني/](https://www.rmg-sa.com/الامتثال-لمعايير-الأمن-السيبراني/)
2. فرح الروسان وديما ابو عليم، أنواع الأمن السيبراني، 17 نوفمبر 2021، أنواع الأمن السيبراني، كانت آخر زيارة للموقع الالكتروني بتاريخ 2023/1/3.
[أنواع الأمن السيبراني/](https://mawdoo3.com/أنواع الأمن السيبراني/)

المصادر والمراجع الأجنبية

A: Books

1. Cohen, J. "Statistical power analysis for the behavioral sciences (rev. ed.) Lawrence Erlbaum Associates." Inc., Hillsdale, NJ, England (1977).
2. Cooper, D.R. & Schindler, P.S. (2014). Business research methods (12th edn). Boston: McGraw-Hill
3. Ecosip. Dialogues autour de la performance en entreprise: les enjeux. Editions L'Harmattan, 1999.
4. Edgeman, Rick. "Excellence models as complex management systems: An examination of the Shingo operational excellence model." Business Process Management Journal (2018).
5. HAJRA BIBI & MAHR MUHAMMAD SAEED AKHTAR, Relationship between Leadership Commitment and Performance of Public Sector Universities of Punjab, Pakistan, 2020.
6. Mardiana, Mardiana, and Puji Endah Purnamasari. "The effect of risk management on financial performance with good corporate governance as a moderation variable." Management and Economics Journal (MEC-J) 2.3 (2018): 257-268.
7. Middleton, Bruce. A history of cyber security attacks: 1980 to present. Auerbach Publications, 2017.
8. Uma, Sekaran. Research methods for business _ a skill-building approach, 4th ed. John Wiley & Sons, Inc, 2003.
9. Whitman, M. E., and H. J. Mattord. "Management of Information Security . Cengage Learning." Inc., Boston, MA 2210 (2019).

B: Periodicals & Journals

1. Alyoshin, C. П., and O. M. Гайтан. Neural network technology of recognition of hacker applications for traffic interception and analysis= Нейромережева технологія розпознавання хакерських додатків для переходу та аналізу трафіка. Diss. Чернігівський національний технічний університет, 2020.
2. Ajis, Andri, et al. "The Influence of Transformational Leadership and HRM Practices on Organization Performance: Organization Trust as a Mediator." Budapest International Research and Critics Institute-Journal (BIRCI-Journal) 5.3 (2022): 18474-18487.
3. Al-rimy, Bander Ali Saleh, et al. "Zero-day aware decision fusion-based model for crypto-ransomware early detection." International Journal of Integrated Engineering 10.6 (2018).
4. Aristotle Onyemaechi ONUMO, A Behavioural Compliance Framework for Effective Cybersecurity Governance and Practice. Examining the interaction of cultural characteristics and cybersecurity governance in fostering organis, 2020.
5. Awan, Mazhar Javed, et al. "Real-time DDoS attack detection system using big data approach." Sustainability 13.19 (2021): 10743.
6. Björck, Fredrik, et al. "Cyber resilience—fundamentals for a definition." New Contributions in Information Systems and Technologies: Volume 1. Springer International Publishing, 2015.
7. Bojjagani, Sriramulu, DR Denslin Brabin, and PV Venkateswara Rao. "PhishPreventer: a secure authentication protocol for prevention of phishing attacks in mobile environment with formal verification." Procedia Computer Science 171 (2020): 1110-1119.

8. Chandra, J. Vijaya, Narasimham Challa, and Sai Kiran Pasupuletti. "Authentication and authorization mechanism for cloud security." *International Journal of Engineering and Advanced Technology* 8.6 (2019): 2072-2078.
9. Dejan Kosutic, *The Impact of Cybersecurity on Competitive Advantage*, A thesis submitted for the degree of Doctorate of Business Administration, Defended on Date December 9, 2021.
10. Dewberry, Chris. *Statistical methods for organizational research: Theory and practice*. Routledge, 2004.
11. Freyhof, Mark. "Cybersecurity of Agricultural Machinery: Exploring Cybersecurity Risks and Solutions for Secure Agricultural Machines." (2022).
12. Giri, Babu Nath, Nitin Jyoti, and M. Avert. "The emergence of ransomware." *AVAR*, Auckland (2006).
13. Haddadpajouh, Hamed, et al. "MV FCC: A multi-view fuzzy consensus clustering model for malware threat attribution." *IEEE Access* 8 (2020): 139188-139198.
14. Han, Dongqi, et al. "DeepAID: interpreting and improving deep learning-based anomaly detection in security applications." *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. 2021.
15. Hu, Fan, Aozhu Chen, and Xirong Li. "Targeted Trojan-Horse Attacks on Language-based Image Retrieval." *arXiv preprint arXiv:2202.03861* (2022).
16. Hussien, Assist Prof Dr Khalid Ali, Assist Prof Dr Sawsen Abdulhadi Mahmood, and Mazin Adnan Abbas. "RPTPA: Random Pattern Technique Based Password Authentication." *Iraqi Journal of Information Technology*. V 9.2 (2018).

17. John W. Wesevich, SERVANT LEADERSHIP IMPACT ON ORGANIZATIONAL PERFORMANCE, Doctoral Study Submitted in Partial Fulfillment of the Requirements for the Degree of Doctor of Business Administration, Liberty University, School of Business, May 2022.
18. Johnny Fadel Rawass, Cybersecurity Strategies to Protect Information Systems in Small Financial Institutions, 2019.
19. Julio C. Rodriguez, Public Servants' Perceptions of the Cybersecurity Posture of the Local Government in Puerto Rico, 2019.
20. Kadhim, R., and M. Gaata. "A hybrid of CNN and LSTM methods for securing web application against cross-site scripting attack." *Indones. J. Electr. Eng. Comput. Sci* 21 (2020): 1022-1029.
21. Khan, Firoz, et al. "A digital DNA sequencing engine for ransomware detection using machine learning." *IEEE Access* 8 (2020): 119710-119719.
22. Latchoumi, T. P., Reddy, M. S., & Balamurugan, K. (2020). Applied machine learning predictive analytics to SQL injection attack detection and prevention. *European Journal of Molecular & Clinical Medicine*, 7(02), 2020.
23. Malik, Asad Waqar, and Zahid Anwar. "Do Charging Stations Benefit from Cryptojacking? A Novel Framework for Its Financial Impact Analysis on Electric Vehicles." *Energies* 15.16 (2022): 5773.
24. Mallik, Avijit. "Man-in-the-middle-attack: Understanding in simple words." *Cyberspace: Jurnal Pendidikan Teknologi Informasi* 2.2 (2019): 109-134.
25. Obeed, Dr. "The quality of institutional performance according to the entrepreneurial management Applied research in the Municipality of Baghdad." *Journal of Contemporary Issues in Business and Government* 27.2 (2021): 6709-6730.
26. Onumo, Aristotle O. A Behavioural Compliance Framework for Effective Cybersecurity Governance and Practice. Examining the interaction of cultural

- characteristics and cybersecurity governance in fostering organisational compliance using case studies. Diss. University of Bradford, 2020.
- 27.Ridwan, Muhammad. "Budapest International Research and Critics Institute- Journal (BIRCI-Journal)." Marriage 28893 (2022): 28903.
- 28.Salahdine, Fatima, and Naima Kaabouch. "Social engineering attacks: A survey." Future Internet 11.4 (2019): 89.
- 29.Salman, Rabia. A study on innovative culture, strategic planning and SMEs performance in Punjab, Pakistan. Diss. Doctoral dissertation, University Utara Malaysia). MCDM framework for green supplier selection. Journal of Cleaner Production, 1, 2017.
- 30.Subramaniam, Thalagawathi Siva. Examining agile leadership style on organizational performance through the mediation of organizational culture: a case study on professional bodies in Malaysia. Diss. University of Wales Trinity Saint David (United Kingdom), 2022.
- 31.Uwakweh, Ozioma IF. Cybersecurity in the Retail Industry: Third Party Implications. Diss. University of Cincinnati, 2020.

C: Articles

1. ANTONIA DIN, DIGITAL CONTENT CREATOR, LAST UPDATED ON FEBRUARY 16, 2022, Why Cybersecurity Is Important for Companies?, <https://heimdalsecurity.com/blog/why-cybersecurity-is-important-for-companies/> , Last visit on 3-1-2023.
2. Astha Oriel, September 28, 2020, Five Types of Cyber Security for Organizational Safety, <https://www.analyticsinsight.net/five-types-cyber-security-organizational-safety/> , Viewed on 3-1-2023.
3. National cyber security centre glossary (2016). Retrieved from <https://www.ncsc.gov.uk/information/ncsc-glossary>, Viewed on 3-1-2023.

أَمَلًا حَقِيقًا

ملحق رقم (1) اداة القياس

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة كربلاء
كلية الادارة والاقتصاد
قسم ادارة الاعمال/ دبلوم عالي ادارة الجودة

تقييم أداة القياس

المتعلقة بمشروع بحث الدبلوم العالي الموسوم:

"تأثير الأمن السيبراني على أداء المنظمة: دراسة استطلاعية لآراء عينة من العاملين في شركة ايرثلنك"

الباحث
طالب الدبلوم العالي
رافد عباس حمود
جامعة كربلاء / كلية الادارة والاقتصاد
07706202875

المشرف
الأستاذ المساعد الدكتورة
اميمة حميد العادلي
جامعة كربلاء/ كلية الإدارة والاقتصاد
07716764784

الموضوع / تقييم أداة قياس

حضرة المحكم المحترم ...

السلام عليكم ورحمة الله وبركاته...

نضع بين أيديكم أداة القياس، التي أعدت لإكمال متطلبات بحث الدبلوم الموسوم (تأثير الأمن السيبراني على أداء المنظمة: دراسة استطلاعية لآراء عينة من العاملين في شركة ايرثلنك)، ولما لجنا بكم الكريم من خبرة وكفاءة علمية عالية في مجال إختصاصكم، أرجوا من حضراتكم الموافقة على تقييم هذا المقياس من ناحية مناسبة وأهمية ووضوح كل فقرة من فقراته المعبرة عن كل بُعد.

مع خالص دعائنا لكم بالتوفيق ومزيداً من التقدم العلمي

الجزء الأول: معلومات عامة

يرجى وضع إشارة (√) للفقرة الملائمة:

1. المركز الوظيفي الحالي:
2. النوع الإجتماعي: ذكر أنثى
3. العمر: 25-18 35-26 45-36 55-46 56 فما فوق
4. التحصيل الدراسي: ماجستير دكتوراه اعدادي دبلوم فني بكالوريوس دبلوم عالي
5. سنوات الخدمة الوظيفية: سنة.
6. القسم أو الشعبة أو الوحدة التي تعمل فيها:
7. عدد الدورات التي دخلتها في مجال الامن السيبراني للثلاث سنوات الاخيرة

الجزء الثاني: متغيرات الدراسة

1. الامن السيبراني: يشير الى النهج والاجراءات المرتبطة بعمليات ادارة المخاطر الامنية التي تتبعها المنظمات والدول لحماية السرية والنزاهة وتوافر البيانات والاصول المستخدمة في الفضاء الالكتروني، يتضمن المفهوم المبادئ التوجيهية والسياسات ومجموعة الضمانات والتقنيات والادوات والتدريب لتوفير افضل حماية لحالة البيئة الالكترونية ومستخدميها (Zdravkovic & Stirna, 2015).

ملاحظات المحكم	مدى وضوح الفقرة		مدى إنتماء الفقرة للبعد		الفقرة
	واضحة	غير واضحة	لا تنتمي	تنتمي	
					1- لدي كلمة مرور قوية تتكون من رموز واحرف وارقام صغيرة وكبيرة..

					2- يتم تبادل ارقام المرور السرية للانظمة الالكترونية بين العاملين في الشركة.
					3- يحدد النظام هوية العاملين في حالة الدخول على البيانات او القيام باي عمليات تعديل عليها.
					4- تعالج الشركة نقاط الضعف في اجهزتها وبرمجياتها من خلال سد الثغرات.
					5- توجد تعليمات ادارية صريحة حول حماية النظام من اي تلاعب او غش.
					6- يمتلك العاملون معرفة بتفاصيل عقوبات نشر الوثائق والمعلومات السرية او افشائها.

ب. الخصوصية:. تشير الى حماية البيانات الشخصية للفراد من اي وسيلة اختراق او تجسس على معلوماتهم الشخصية.

ملاحظات المحكم	مدى وضوح الفقرة		مدى إنتماء الفقرة للبعد		الفقرة
	واضحة	غير واضحة	لا تنتمي	تنتمي	
					1-تقوم ادارة الشركة بمراجعة صلاحيات المستخدمين على فترات منتظمة.
					2-واجه اختراقات متكررة على بريدي الالكتروني.
					3-تعتمد ادارة الشركة عدة تقنيات مثل: المصادقة والترخيص والتشفير لحماية الانظمة والبيانات الحساسة.
					4-يتم تشغيل وتحديث جدار الحماية باستمرار لمنع المتسللين من الوصول للبيانات الشخصية او بيانات الشركة.

					5-تتبنى الشركة سياسات امن سيبراني بمعايير عالمية للحد من حالات التجسس والتخريب الرقمي.
					6-توجه الشركة المستخدمين من خدماتها وانظمتها نحو طرق حماية وامن المعلومات.
ج. التعزيز: ويشير الى جوانب التعزيز الامني والحماية لكل الانظمة التقنية والخدمات الالكترونية من اي تهديدات محتملة ويكون ذلك من خلال رفع جودة التعزيز الامني التقني للبنية التحتية لتكنولوجيا المعلومات في الشركة.					
ملاحظات المحكم	مدى وضوح الفقرة		مدى إنتماء الفقرة للبعد		الفقرة
	واضحة	غير واضحة	لا تنتمي	تنتمي	
					1-تتم مراقبة العاملين للتأكد من تطبيق السياسات والاجراءات الوقائية لمنع تسريب المعلومات.
					2-تستخدم برامج مكافحة الفيروسات والمتجسسات بشكل دوري في اجهزة الشركة لحمايتها من البرامج الضارة.
					3-تحمي الشركة انظمتها التشغيلية باعتماد برامج متطورة.
					4-توجد اليات تخزين امنه للوثائق الى جانب وجود نسخ احتياطية (back up) لكافة ملفات ومعلومات الشركة في اقراص صلبة او سحابة خاصة بالشركة.
					5-تقوم الشركة بمراجعة البيانات والمعلومات المتوافرة على شبكتها من اجل اصلاحها في حال تعرضها للاختراقات السيبرانية.
					6- تحذف الشركة البيانات التالفة التي تعرضت لهجمات سيبرانية.

2. اداء المنظمة: ويشير الى الغايات التي ترغب اي منظمة في الوصول اليها بكفاءة وفاعلية (محمد، 2018: 78).

أ. الكفاءة: الاستخدام الامثل للموارد المتاحة للمنظمة في تحقيق اهدافها التي تسعى لتحقيقها.					
ملاحظات المحكم	مدى وضوح الفقرة		مدى إنتماء الفقرة للبعد		الفقرة
	واضحة	غير واضحة	لا تنتمي	تنتمي	
					1-ان الاستثمار الامثل للموارد المتاحة في الشركة تؤدي الى اغناء اعمالها بالمزيد من الخدمات التنافسية
					2-تسعى الشركة الى تحقيق اهدافها في تعزيز الميزة التنافسية من خلال تطوير عملياتها وخلق منتجات وخدمات خاصة بها وقادرة على اضافة مخرجات كفاءة للعمليات الانتاجية نسبة الى مدخلاتها.
					3-تتحقق الخطط الانتاجية الخاصة بعمليات الشركة في تطوير الخدمات الجديدة بصورة كفاءة.
					4-تسهم التقنيات المستعملة في تخطيط وتطوير الخدمات الجديدة في زيادة معدلات ارباح الشركة وزيادة معدلات العوائد على الاستثمار وحق الملكية ومعدلات دوران راس المال

ب. الفاعلية: المعيار الذي يعكس درجة نجاح المنظمة في تحقيق اهدافها.					
ملاحظات المحكم	مدى وضوح الفقرة		مدى إنتماء الفقرة للبعد		الفقرة
	واضحة	غير واضحة	لا تنتمي	تنتمي	
					1-تمتلك الشركة القدرة على تطوير خدمات جديدة اكثر في سبيل تحقيق اهدافها وتوجهاتها.

					2-تسعى الشركة الى تحقيق رضا جميع الاطراف التي لها علاقة بتقديم الخدمات من اجل تحقيق الفاعلية في عمليات تخطيط وتطوير الخدمات الجديدة.
					3-تعمل كل الوحدات او النظم الفرعية باتجاه واحد في سبيل تحقيق اهداف الشركة.
					4-تسهم التقنية المستخدمة لتخطيط وتطوير خدمات جديدة تدعم زيادة القيمة الاجمالية للشركة.

هل يوجد أي ملاحظات أخرى تدعم بها دراستنا لطفاً؟

.....

.....

.....

.....

.....

.....

.....

الإسم واللقب العلمي:

الإختصاص العام والدقيق:

المنصب ومكان العمل:

معلومات الاتصال:

التاريخ:

التوقيع:

ملحق رقم (2) أسماء السادة محكمي أداة القياس

ت	اسم المحكم	اللقب العلمي	التخصص العام	التخصص الدقيق	مكان العمل
1	أ.د. خالد علي حسين المياح	استاذ دكتور	علوم حاسبات	الخوارزميات المتوازية في امن المعلومات والذكاء الصناعي	رئيس قسم علوم الحاسبات/ عضو الفريق الوزاري للتعليم الالكتروني و التحول الرقمي/ الجامعة المستنصرية.
2	أ.د. فيصل علوان الطائي	استاذ دكتور	معلومات وتقنيات معرفة	نظم معلومات وإدارة معرفة	قسم إدارة الاعمال/ كلية الإدارة والاقتصاد/ جامعة كربلاء.
3	أ.د. ميثاق هاتف الفتلاوي	استاذ دكتور	إدارة اعمال	سلوك تنظيمي ونظرية منظمة	قسم إدارة الاعمال/ كلية الإدارة والاقتصاد/ جامعة كربلاء.
4	أ.م.د. احمد عبدالله امانة	استاذ مساعد دكتور	إدارة اعمال	إدارة استراتيجية وإدارة معرفة	قسم إدارة الاعمال/ كلية الإدارة والاقتصاد/ جامعة كربلاء.
5	أ.م.د. بلال عصام عبد الرزاق	استاذ مساعد دكتور	هندسة الالكترون واتصالات	النظم الالكترونية المايكروية الرقمية	رئيس قسم تكنولوجيا المعلومات والاتصالات/ مركز وزارة الصناعة والمعادن.
6	أ.م.د. سناء جواد كاظم	أستاذ مساعد دكتور	إدارة اعمال	إدارة معرفة	قسم إدارة الاعمال/ كلية الإدارة والاقتصاد/ جامعة القادسية.
7	أ.م.د. يزن سالم محمد	أستاذ مساعد دكتور	إدارة اعمال	سلوك تنظيمي	قسم إدارة الاعمال/ كلية الإدارة والاقتصاد/ جامعة كربلاء.
8	د. رافت عارف عبدالحسين	خبير	تكنولوجيا معلومات واتصالات	تقنيات العمليات	قسم تكنولوجيا المعلومات والاتصالات/ مركز وزارة الصناعة والمعادن.

● ملاحظة: جرى ترتيب أسماء الخبراء وفقاً للقب العلمي أولاً ثم هجائياً ضمن كل لقب.

ملحق رقم (3) الاستبانة

جامعة كربلاء

كلية الإدارة والاقتصاد

الدراسات العليا/ دبلوم عالي ادارة الجودة

تأثير الأمن السيبراني على أداء المنظمة: دراسة استطلاعية لآراء عينة من العاملين في شركة (ايرثلنك)

الموضوع/ استبانة

إلى السيدات والسادة المحترمون (العاملون في شركة ايرثلنك)

السلام عليكم ورحمة الله وبركاته...

نضع بين ايديكم الاستبانة التي أعدت لقياس متغيرات البحث الموسوم (تأثير الأمن السيبراني على أداء المنظمة: دراسة استطلاعية لآراء عينة من العاملين في شركة ايرثلنك)، وهي جزء من متطلبات نيل درجة الدبلوم العالي في تخصص إدارة الجودة وأملنا كبير في تعاونكم معنا في القراءة الدقيقة لفقرات الاستبيان وإجاباتكم عنها من واقع ما تمتلكون من خبرة ومقدرة علمية، وأن ما تقدمونه من إجابات دقيقة وموضوعية سيكون لها التأثير المفيد على نتائج البحث.

شاكرين تعاونكم و متمنين لكم دوام التوفيق.

ويرجى التفضل بقراءة الملاحظات الآتية:

1. إن إجاباتكم سوف لن تستخدم إلا لأغراض البحث العلمي فلا داعي لذكر الاسم رجاء أو التوقيع على الاستبانة.
2. رأيك الموضوعي الدقيق هو المطلوب، إذ ليس هناك إجابات صحيحة أو خاطئة.
3. ستجد أمام كل فقرة (5) بدائل تتراوح بين (اتفق تماما، اتفق، محايد، لا اتفق، لا اتفق تماما)، يرجى منك اختيار واحدة منها والتي تُعبّر عن وجهة نظرك.
4. يرجى عدم ترك أي فقرة دون إجابة.

المشرف

أ.م.د. اميمة حميد العادلي

omaima.h@uokerbala.edu.iq

الباحث

رافد عباس حمود

eng.rafid2021@gmail.com

***مطلوب**

1. المركز الوظيفي الحالي *
2. النوع الاجتماعي * حدد دائرة واحدة فقط
 - ذكر
 - أنثى
3. الفئة العمرية * حدد دائرة واحدة فقط
 - 25-18
 - 35-26
 - 45-36
 - 55-46
 - 55 فأكثر
4. التحصيل الدراسي * حدد دائرة واحدة فقط
 - اعدادية
 - دبلوم فني
 - بكالوريوس
 - دبلوم عالي
 - ماجستير
 - دكتوراه
5. سنوات الخدمة الوظيفية *
6. عدد الدورات التي دخلتها في مجال الأمن السيبراني للثلاث سنوات الأخيرة *

أسئلة المتغير الأول (الأمن السيبراني)

1. لدي كلمة مرور قوية تتكون من رموز وأحرف وأرقام صغيرة وكبيرة *
 - اتفق تماما
 - اتفق
 - محايد
 - لا اتفق
 - لا اتفق تماما
2. يتم تبادل أرقام المرور السرية للأنظمة الالكترونية بين العاملين في الشركة *
 - اتفق تماما
 - اتفق
 - محايد
 - لا اتفق

- 0 لا اتفق تماما
3. لمديري شبكات الشركة القدرة على اعطاء الصلاحيات المختلفة للمستخدمين (قراءة فقط، تعديل، قراءة وكتابة) باستخدام الخصائص التي توفرها الأنظمة المستخدمة في الشركة*
- 0 اتفق تماما
- 0 اتفق
- 0 محايد
- 0 لا اتفق
- 0 لا اتفق تماما
4. تفرض الشركة على موظفيها تبديل كلمات المرور بشكل دوري*
- 0 اتفق تماما
- 0 اتفق
- 0 محايد
- 0 لا اتفق
- 0 لا اتفق تماما
5. توجد تعليمات إدارية صريحة حول حماية النظام من اي تلاعب أو غش*
- 0 اتفق تماما
- 0 اتفق
- 0 محايد
- 0 لا اتفق
- 0 لا اتفق تماما
6. يمتلك العاملون معرفة بتفاصيل عقوبات نشر الوثائق والمعلومات السرية أو افشائها*
- 0 اتفق تماما
- 0 اتفق
- 0 محايد
- 0 لا اتفق
- 0 لا اتفق تماما
7. تقوم إدارة الشركة بمراجعة صلاحيات المستخدمين على فترات منتظمة*
- 0 اتفق تماما
- 0 اتفق
- 0 محايد
- 0 لا اتفق
- 0 لا اتفق تماما
8. واجه اختراقات متكررة على بريدي الالكتروني*

- 0 اتفق تماما
- 0 اتفق
- 0 محايد
- 0 لا اتفق
- 0 لا اتفق تماما
9. تعتمد إدارة الشركة عدة تقنيات مثل: المصادقة والترخيص والتشفير لحماية الأنظمة والبيانات الحساسة*
- 0 اتفق تماما
- 0 اتفق
- 0 محايد
- 0 لا اتفق
- 0 لا اتفق تماما
10. يتم تشغيل وتحديث جدار الحماية باستمرار لمنع المتسللين من الوصول للبيانات الشخصية أو بيانات الشركة*
- 0 اتفق تماما
- 0 اتفق
- 0 محايد
- 0 لا اتفق
- 0 لا اتفق تماما
11. تتبنى الشركة سياسات أمن سيراني بمعايير عالمية للحد من حالات التجسس والتخريب الرقمي*
- 0 اتفق تماما
- 0 اتفق
- 0 محايد
- 0 لا اتفق
- 0 لا اتفق تماما
12. تقيم الشركة ورش عمل ودورات تدريبية متخصصة للمستفيدين حول طرق حماية وأمن المعلومات*
- 0 اتفق تماما
- 0 اتفق
- 0 محايد
- 0 لا اتفق
- 0 لا اتفق تماما
13. تعتمد الشركة وسائل لتحديد الموظفين الذين لديهم صلاحية الوصول إلى موقع معالجة وخرن البيانات*

- 0 اتفق تماما
- 0 اتفق
- 0 محايد
- 0 لا اتفق
- 0 لا اتفق تماما
14. تستخدم برامج مكافحة الفيروسات والمتجسّسات المرخصة بشكل دوري في أجهزة الشركة لحماية من البرامج الضارة*
- 0 اتفق تماما
- 0 اتفق
- 0 محايد
- 0 لا اتفق
- 0 لا اتفق تماما
15. يتم حماية الأنظمة التشغيلية (Operating Systems OS) باستخدام أجهزة (Hardware) حماية متطورة وبرامجيات (Software) حماية، أو اعتماد آليات من تصميم الشركة ذاتها*
- 0 اتفق تماما
- 0 اتفق
- 0 محايد
- 0 لا اتفق
- 0 لا اتفق تماما
16. توجد آليات تخزين آمنة للوثائق إلى جانب وجود نسخ احتياطية (back up) لكافة ملفات ومعلومات الشركة في اقراص صلبة أو سحابة خاصة بالشركة*
- 0 اتفق تماما
- 0 اتفق
- 0 محايد
- 0 لا اتفق
- 0 لا اتفق تماما
17. لدى الشركة وسائل لمراقبة البيانات وتحديد المخترق منها وبالتالي يمكن عزلها ومحاولة علاجها*
- 0 اتفق تماما
- 0 اتفق
- 0 محايد
- 0 لا اتفق
- 0 لا اتفق تماما

18. تُحدث إدارة الشركة باستمرار آليات تعزيز حماية شبكاتها من خلال مواكبة الاتجاهات والمعايير العالمية المتخصصة بهذا المجال*

- 0 اتفق تماما
0 اتفق
0 محايد
0 لا اتفق
0 لا اتفق تماما

المتغير الثاني (التابع: أداء المنظمة)

1. تسعى الشركة في استثمارها للموارد المتاحة إلى اغناء أعمالها بالمزيد من الخدمات التنافسية*

- 0 اتفق تماما
0 اتفق
0 محايد
0 لا اتفق
0 لا اتفق تماما

2. تسعى الشركة الى تحقيق اهدافها في تعزيز الميزة التنافسية من خلال تطوير عملياتها وخلق منتجات وخدمات خاصة بها قادرة على اضافة مخرجات كفاءة للعمليات الانتاجية نسبة إلى مدخلاتها*

- 0 اتفق تماما
0 اتفق
0 محايد
0 لا اتفق
0 لا اتفق تماما

3. تتحقق الخطط الانتاجية الخاصة بعمليات الشركة في تطوير الخدمات الجديدة بصورة كفاءة*

- 0 اتفق تماما
0 اتفق
0 محايد
0 لا اتفق
0 لا اتفق تماما

4. تسهم التقنيات المستعملة في تخطيط وتطوير الخدمات الجديدة في زيادة معدلات أرباح الشركة وزيادة معدلات العوائد على الاستثمار وحق الملكية ومعدلات دوران رأس المال*

- 0 اتفق تماما
0 اتفق

- 0 محايد
- 0 لا اتفق
- 0 لا اتفق تماما
5. تمتلك الشركة القدرة على تطوير خدمات جديدة أكثر في سبيل تحقيق أهدافها وتوجهاتها*
- 0 اتفق تماما
- 0 اتفق
- 0 محايد
- 0 لا اتفق
- 0 لا اتفق تماما
6. تسعى الشركة إلى تحقيق رضا جميع الاطراف التي لها علاقة بتقديم الخدمات من أجل تحقيق الفاعلية في عمليات تخطيط وتطوير الخدمات الجديدة*
- 0 اتفق تماما
- 0 اتفق
- 0 محايد
- 0 لا اتفق
- 0 لا اتفق تماما
7. تعمل كل الوحدات أو النظم الفرعية باتجاه واحد في سبيل تحقيق أهداف الشركة*
- 0 اتفق تماما
- 0 اتفق
- 0 محايد
- 0 لا اتفق
- 0 لا اتفق تماما
8. تسهم التقنية المستخدمة لتخطيط وتطوير خدمات جديدة تدعم زيادة القيمة الاجمالية للشركة*
- 0 اتفق تماما
- 0 اتفق
- 0 محايد
- 0 لا اتفق
- 0 لا اتفق تماما

ملحق رقم (4) قيم T الجدولية

Upper critical values of Student's t distribution with ν degrees of freedom

ν	Probability of exceeding the critical value					
	0.10	0.05	0.025	0.01	0.005	0.001
1.	3.078	6.314	12.706	31.821	63.657	318.313
2.	1.886	2.920	4.303	6.965	9.925	22.327
3.	1.638	2.353	3.182	4.541	5.841	10.215
4.	1.533	2.132	2.776	3.747	4.604	7.173
5.	1.476	2.015	2.571	3.365	4.032	5.893
6.	1.440	1.943	2.447	3.143	3.707	5.208
7.	1.415	1.895	2.365	2.998	3.499	4.782
8.	1.397	1.860	2.306	2.896	3.355	4.499
9.	1.383	1.833	2.262	2.821	3.250	4.296
10.	1.372	1.812	2.228	2.764	3.169	4.143
11.	1.363	1.796	2.201	2.718	3.106	4.024
12.	1.356	1.782	2.179	2.681	3.055	3.929
13.	1.350	1.771	2.160	2.650	3.012	3.852
14.	1.345	1.761	2.145	2.624	2.977	3.787
15.	1.341	1.753	2.131	2.602	2.947	3.733
16.	1.337	1.746	2.120	2.583	2.921	3.686
17.	1.333	1.740	2.110	2.567	2.898	3.646
18.	1.330	1.734	2.101	2.552	2.878	3.610
19.	1.328	1.729	2.093	2.539	2.861	3.579
20.	1.325	1.725	2.086	2.528	2.845	3.552
21.	1.323	1.721	2.080	2.518	2.831	3.527
22.	1.321	1.717	2.074	2.508	2.819	3.505
23.	1.319	1.714	2.069	2.500	2.807	3.485
24.	1.318	1.711	2.064	2.492	2.797	3.467
25.	1.316	1.708	2.060	2.485	2.787	3.450
26.	1.315	1.706	2.056	2.479	2.779	3.435
27.	1.314	1.703	2.052	2.473	2.771	3.421
28.	1.313	1.701	2.048	2.467	2.763	3.408
29.	1.311	1.699	2.045	2.462	2.756	3.396
30.	1.310	1.697	2.042	2.457	2.750	3.385
31.	1.309	1.696	2.040	2.453	2.744	3.375
32.	1.309	1.694	2.037	2.449	2.738	3.365
33.	1.308	1.692	2.035	2.445	2.733	3.356
34.	1.307	1.691	2.032	2.441	2.728	3.348
35.	1.306	1.690	2.030	2.438	2.724	3.340
36.	1.306	1.688	2.028	2.434	2.719	3.333
37.	1.305	1.687	2.026	2.431	2.715	3.326
38.	1.304	1.686	2.024	2.429	2.712	3.319
39.	1.304	1.685	2.023	2.426	2.708	3.313
40.	1.303	1.684	2.021	2.423	2.704	3.307
41.	1.303	1.683	2.020	2.421	2.701	3.301

ملحق رقم (5) قيم F الجدولية

Critical Values of the *F*-Distribution: $\alpha = 0.01$

Denom. d.f.	Numerator Degrees of Freedom									
	1	2	3	4	5	6	7	8	9	10
1	4052.181	4999.500	5403.352	5624.583	5763.650	5858.986	5928.356	5981.070	6022.473	6055.847
2	98.503	99.000	99.166	99.249	99.299	99.333	99.356	99.374	99.388	99.399
3	34.116	30.817	29.457	28.710	28.237	27.911	27.672	27.489	27.345	27.229
4	21.198	18.000	16.694	15.977	15.522	15.207	14.976	14.799	14.659	14.546
5	16.258	13.274	12.060	11.392	10.967	10.672	10.456	10.289	10.158	10.051
6	13.745	10.925	9.780	9.148	8.746	8.466	8.260	8.102	7.976	7.874
7	12.246	9.547	8.451	7.847	7.460	7.191	6.993	6.840	6.719	6.620
8	11.259	8.649	7.591	7.006	6.632	6.371	6.178	6.029	5.911	5.814
9	10.561	8.022	6.992	6.422	6.057	5.802	5.613	5.467	5.351	5.257
10	10.044	7.559	6.552	5.994	5.636	5.386	5.200	5.057	4.942	4.849
11	9.646	7.206	6.217	5.668	5.316	5.069	4.886	4.744	4.632	4.539
12	9.330	6.927	5.953	5.412	5.064	4.821	4.640	4.499	4.388	4.296
13	9.074	6.701	5.739	5.205	4.862	4.620	4.441	4.302	4.191	4.100
14	8.862	6.515	5.564	5.035	4.695	4.456	4.278	4.140	4.030	3.939
15	8.683	6.359	5.417	4.893	4.556	4.318	4.142	4.004	3.895	3.805
16	8.531	6.226	5.292	4.773	4.437	4.202	4.026	3.890	3.780	3.691
17	8.400	6.112	5.185	4.669	4.336	4.102	3.927	3.791	3.682	3.593
18	8.285	6.013	5.092	4.579	4.248	4.015	3.841	3.705	3.597	3.508
19	8.185	5.926	5.010	4.500	4.171	3.939	3.765	3.631	3.523	3.434
20	8.096	5.849	4.938	4.431	4.103	3.871	3.699	3.564	3.457	3.368
21	8.017	5.780	4.874	4.369	4.042	3.812	3.640	3.506	3.398	3.310
22	7.945	5.719	4.817	4.313	3.988	3.758	3.587	3.453	3.346	3.258
23	7.881	5.664	4.765	4.264	3.939	3.710	3.539	3.406	3.299	3.211
24	7.823	5.614	4.718	4.218	3.895	3.667	3.496	3.363	3.256	3.168
25	7.770	5.568	4.675	4.177	3.855	3.627	3.457	3.324	3.217	3.129
26	7.721	5.526	4.637	4.140	3.818	3.591	3.421	3.288	3.182	3.094
27	7.677	5.488	4.601	4.106	3.785	3.558	3.388	3.256	3.149	3.062
28	7.636	5.453	4.568	4.074	3.754	3.528	3.358	3.226	3.120	3.032
29	7.598	5.420	4.538	4.045	3.725	3.499	3.330	3.198	3.092	3.005
30	7.562	5.390	4.510	4.018	3.699	3.473	3.304	3.173	3.067	2.979
31	7.530	5.362	4.484	3.993	3.675	3.449	3.281	3.149	3.043	2.955
32	7.499	5.336	4.459	3.969	3.652	3.427	3.258	3.127	3.021	2.934
33	7.471	5.312	4.437	3.948	3.630	3.406	3.238	3.106	3.000	2.913
34	7.444	5.289	4.416	3.927	3.611	3.386	3.218	3.087	2.981	2.894
35	7.419	5.268	4.396	3.908	3.592	3.368	3.200	3.069	2.963	2.876
36	7.396	5.248	4.377	3.890	3.574	3.351	3.183	3.052	2.946	2.859
37	7.373	5.229	4.360	3.873	3.558	3.334	3.167	3.036	2.930	2.843
38	7.353	5.211	4.343	3.858	3.542	3.319	3.152	3.021	2.915	2.828
39	7.333	5.194	4.327	3.843	3.528	3.305	3.137	3.006	2.901	2.814
40	7.314	5.179	4.313	3.828	3.514	3.291	3.124	2.993	2.888	2.801
41	7.296	5.163	4.299	3.815	3.501	3.278	3.111	2.980	2.875	2.788
42	7.280	5.149	4.285	3.802	3.488	3.266	3.099	2.968	2.863	2.776
43	7.264	5.136	4.273	3.790	3.476	3.254	3.087	2.957	2.851	2.764
44	7.248	5.123	4.261	3.778	3.465	3.243	3.076	2.946	2.840	2.754
45	7.234	5.110	4.249	3.767	3.454	3.232	3.066	2.935	2.830	2.743

Abstract:

Abstract

The research aims to shed light on the variable of cybersecurity and its impact on the performance of the organization by conducting the research on a sample of employees at the headquarters of the Earthlink Company in Baghdad. The researched company adopts cybersecurity applications and invests them in supporting its business?), as cybersecurity was used as an independent variable with three dimensions (confidentiality, privacy and enhancement) and the dependent variable is the performance of the organization and it is determined by two dimensions (efficiency and effectiveness), and in order to achieve this, the research adopted the descriptive approach, and it was The intentional sample includes workers in the field of information technology in the researched company, and the questionnaire was used as a tool for data collection. Cronbach Alpha) to measure the stability and validity of the scale, simple correlation analysis and simple linear regression based on the statistical analysis program (SPSS V.26), and a total of A number of conclusions, the most important of which was the presence of a significant impact relationship of cybersecurity on the performance of the organization, and that cybersecurity explains a specific percentage of changes in the performance of the organization, and it was also shown that the searched company adopts cybersecurity through its interest in (confidentiality, privacy, and enhancement). In its work, and as the researcher reached a set of recommendations, the most important of which was to increase interest in confidentiality, especially the workers' awareness of the importance of not exchanging secret password numbers for the electronic systems they work on, as well as paying more attention to the production plans for the organization's operations because of their role in developing new services and being affected in a way Positive on the efficiency of the organization.

Keywords: cyber security, organization performance.

Ministry of Higher Education
And Scientific Research
University of Kerbala
College of Administration and Economic
Department of Business Administration



The impact of cyber security in organization performance
**An exploratory study of the opinions of a sample of employees at EarthLink
Company**

**Research submitted to the council of the College of Administration and
Economics/ University of Kerbala as part of the requirements for degree a
higher diploma in Quality Management**

Written By:

Rafed Abaas Hmood

Supervised By:

Assistant Professor

Dr. Omaima Hamid Abdullah