



وزارة التعليم العالي والبحث العلمي

الجامعة التقنية الوسطى

الكلية التقنية الإدارية - بغداد

وقائع المؤتمر العلمي التخصصي الرابع

للكلية التقنية الإدارية - بغداد

للمدة من

2018 / 11 / 29 - 28

تحت شعار

الإبداع الإداري لتحقيق الرؤية المستقبلية

لمنظمات الأعمال

المجلد الثاني / رقم الإصدار (642)

البحوث المنشورة محكمة

الفهرست المجلد الثاني

المحور المعلوماتي			
358-370	م. انهار خير الدين محمد م. نعمة عبد الله الفخري	تصميم نظام معلومات لدعم تطبيق الادارة الالكترونية الذكية في الشركات المساهمة	47
371-383	أ.م. د. احمد ذياب احمد م. د. بشرى خريبط جاسم	اهمية استعمال تكنولوجيا المعلومات والاحصاء في المؤسسات الحكومية	48
384-393	Dr. Sabah F. Abdulhussein	Statistical Study on Causes f Begging Spread Phenomenon in Baghdad From Academic Point of View	49
394-403	A.P.Dr. Maisa,a Abid Ali A.P. Muntaha Khudair Abbas	Steganography Secret Message based on Image Sharpening Using 2D Hear Wavelet Transform	50
404-426	أ.م. د. محمد حسن رشم المهندس د. مؤيد اكرم ارسلان م.م. سناء علي جبر	متطلبات نجاح الادارة الحديثة الالكترونية وتطبيقاتها في الدوائر الحكومية	51
427-436	أ.م. د. أسماعيل هادي جلوب م. بلسم مصطفى شفيق م. محمد فاضل ابراهيم	أيجاد زمن البقاء باستخدام دالة كامبل للتوزيع الثنائي الاسي المشترك لعدة مختبرات لمرض الفشل الكلوي /دراسة تطبيقية	52
437-447	أ.م. د. وليد عبد الله أرحيمه الباحثة هديل صادق احمد	تصنيف مجاميع البيانات الطبية باستخدام خوارزمية الشبكات	53
448-456	أ.م. د. أسماعيل هادي جلوب الباحثة أسماء نجم عبد الله	استخدام الطرائق الذكية لتشخيص مرض سرطان الدم النخاعي من خلال نماذج الانحدار	54
457-480	أ.د. فريد مجيد عبد أ.م. د. نشأت جاسم محمد م.م. نادية عبدالله	تقويم جودة نظام ادارة التعليم الالكتروني (Moodle) من جهة نظر الطلبة /دراسة تطبيقية في الكلية التقنية الادارية / بغداد	55
481-499	م.م. بشرى علي زينل م.م. سحر جلال فتاح	دور أمن المعلومات في الحصول على ثقة الزبون / دراسة استطلاعية لأراء عينة من العاملين في شركات كورك وأسيا سيل ونوروز تيليكوم للاتصالات / اربيل	56
500-515	م. د. هدى عبد الرحيم حسين	واقع البنية التحتية لتقانة المعلومات/دراسة ميدانية في شركة الحكماء لصناعة الادوية والمستلزمات الطبية في الموصل	57

دور أمن المعلومات في الحصول على ثقة الزبون/ دراسة استطلاعية لآراء عينة من العاملين في شركات كورك واسياسيل ونوروز تيليكم للاتصالات/ أربيل

The role of information security in obtaining the customer's trust/ an exploratory study for a sample of workers' views at Korek, Nowroz and Asiacell companies for telecommunication/Erbil

م. سحر جلال فتاح

م.م بشرى علي زينل

كلية العلوم الادارية والمالية
جامعة جيهان - اربيل، العراق، أربيل

Abstract

This study aims to identify the concept of information security since its one of the important topics that is usually omitted by our organizations, in addition to, measuring the relationship and the effect between information security and customer's trust in telecommunication companies by using regression and correlation statistics. And This study is considered important because it deals with one of the vital topics nowadays, namely: how to make it possible to use information security in various types of organizations and its relationship with customers' trust.

To achieve the goals of the study we distributed 61 questionnaires on a sample of employees at Korek and Asia cell and Nowroz companies for telecommunications, after that we analyzed the results by the SPSS program, by testing the correlation and regression between each of the variables of the study. We can summarize the research problem with the following research questions: Do the studied telecommunication companies have a sufficient infrastructure that can be used manage the companies information security and gain customers long range trust? Do the telecommunication companies have sufficient services that satisfies the customers and gain the competitive advantage? And the study ended with a set of conclusions, the most important ones are The company is honest when it comes to the promises that they give to customers, since most of the responder's opinions agreed with this. And there is a significant correlation between information security and customers' trust, besides that information security have an effect on the customer trust, based on the results of ANOVA analysis for regression.

Based on the conclusions the study ended with a set of recommendations, such as both of Korek and Asia cell and Nawroz companies should give more attention to build a satisfactory applications of information security for the customer by updating their technologies and developing the existing systems to be more secured and comfortable.

Key words : information security, information systems, customer trust, information, data

المستخلص

تهدف هذه الدراسة إلى التعرف على مفهوم أمن المعلومات لكونه أحد المواضيع المهمة التي عادة ما يتم الأغفال عنها من قبل المنظمات، بالإضافة إلى قياس العلاقة والاثار ما بين أمن المعلومات وثقة الزبون في شركات الاتصالات عن طريق استخدام الانحدار والارتباط، وتتبع أهمية هذه الدراسة من تركيزها على أحد الموضوعات الحيوية في الوقت الحاضر ألا وهي كيفية استخدام أمن المعلومات في مختلف أنواع المنظمات وعلاقتها بثقة الزبون ومن أجل تحقيق أهداف الدراسة تم توزيع 61 استمارة استبيان على عينة من العاملين في شركات كورك تيليكوم، آسيا سيل، ونوروز للاتصالات في اربيل ، بعد ذلك تم تحليل النتائج باستخدام برنامج SPSS ، من خلال استخدام معاملات الارتباط والانحدار مابين متغيرات الدراسة. تتلخص مشكلة البحث من خلال التساؤلات البحثية الآتية: هل لدى شركات الاتصالات المبحوثة بنية تحتية كفوءة يمكن استخدامها في إدارة أمن معلومات الشركات وكسب ثقة الزبائن على المدى البعيد؟ هل لدى شركات الاتصالات خدمات كفوءة ترضي الزبائن وتساعد على الحصول على الميزة التنافسية؟، واختتمت الدراسة بمجموعة من الاستنتاجات ، أهمها أن الشركات المذكورة صادقة على الاغلب عندما يتعلق الأمر بالوعود التي تقدمها لزبائنهم ، وتبين أيضاً أن هنالك علاقة ارتباط معنوية مابين أمن معلومات الشركات وثقة الزبائن ، إلى جانب ذلك تبين وجود تأثير لأمن المعلومات على ثقة الزبون بالاعتماد على نتائج تحليل انحدار ANOVA واستناداً إلى الاستنتاجات ، خرجت الدراسة بمجموعة من التوصيات منها ضرورة ايلاء اهتمام اكبر من قبل الشركات المبحوثة ببناء تطبيقات أمن معلومات مرضية للزبون من خلال تحديث تقاناتها الحالية بالإضافة الى تطوير الأنظمة الحالية لتكون أكثر سهولة وأمناً.

الكلمات المفتاحية: أمن المعلومات، نظم المعلومات، ثقة الزبون، المعلومات، البيانات

المقدمة

يعد امن المعلومات احد اهم العوامل التي تؤدي الى الحصول على ثقة الزبون في المنظمات ومن خلال استخدام أمن المعلومات بالامكان ايجاد حلول على الاغلب لجميع المشاكل التقنية بالإضافة الى استغلال كافة الفرص التي تواجه المنظمة، وبسبب كون المعلومات من الموارد المهمة ،فانه

بالامكان القيام بتوظيفها والاستفادة منها سواءً داخل المنظمة او في بيئتها الخارجية، وبالاتماد على ما سبق فعلى المنظمات ان تبحث دوماً عن طرق مختلفة لرفع مستوى جودة قراراتها وذلك يتم من خلال الحفاظ على أمانة المعلومات المتوفرة لديها وازافة خصوصية كاملة لكافة بيانات زبائنها، والشركات وخصوصاً التي تعمل في مجال الاتصالات تعتمد بشكل كبير على استخدام ونشر انواع مختلفة من التقنيات التي تستهدف ادارة رأس المال الفكري لديها واستخدام انظمة معلومات تتمتع باعلى مستويات الأمان والسرية والخصوصية، من خلال تجميع جميع البيانات المهمة في النظام وبعد ذلك القيام بمعالجتها وتحويلها الى معلومات قابلة للاستخدام في اتخاذ جميع القرارات الاستراتيجية والتكتيكية من قبل قادة المنظمة. من جانب آخر فإن ثقة الزبون تعد من المفاهيم المرتبطة بالعديد من المفاهيم الاخرى، مثال على ذلك سمعة المنظمة التي تعتمد على مدى ثقة الزبائن بتنفيذها لكافة وعودها لها في المستقبل ، وبما ان معظم الزبائن لديهم اهتمام كبير بالحفاظ على سلامة وخصوصية معلوماتهم الشخصية، وقد تم تقسيم هيكلية البحث الى ثلاثة محاور، المحور الاول منهجية البحث، اما المحور الثاني فتضمن الجانب النظري بمتغيريه الاول أمن المعلومات، والثاني ثقة الزبون، اما المحور الثالث فتضمن الجانب العملي للدراسة وتحليل اجابات عينة البحث، في حين تضمن المحور الرابع الاستنتاجات والتوصيات التي خرج بها البحث.

المحور الأول منهجية البحث

تتضمن منهجية البحث الفقرات الآتية:

1.1 مشكلة البحث : يمكن توضيح مشكلة البحث من خلال التساؤلات البحثية الآتية:

- هل تمتلك الشركات المبحوثة بنية تحتية أمنية كفوءة يمكن استخدامها لادارة كافة معلوماتها والحصول على ثقة الزبون على المدى البعيد؟
- هل تمتلك الشركات المبحوثة الخدمات الكافية التي ترضي حاجات الزبائن وتساعد الشركات من الجانب الاخر على الحصول على الميزة التنافسية المستدامة ؟
- هل تمتلك الشركات المبحوثة بنية تحتية أمنية قوية تحافظ على معلومات الزبون وسرية وخصوصية كافة المعلومات الشخصية الخاصة به؟

1.2 اهمية البحث : والتي يمكن ايضاحها من خلال التالي:

- جاء هذا البحث للتركيز على أمن المعلومات والذي يعد من المواضيع التي عادة ما يتم الأغفال عنها خصوصاً في الشركات الخاصة بالاتصالات.
- تسليط الضوء اكثر على العلاقة مابين متغيرات البحث والتي تتمثل بأمن المعلومات وثقة الزبون.
- الاستفادة من نتائج البحث لغرض تطوير وتحسين الانظمة المستخدمة من قبل الشركات المذكورة.

1.3 اهداف البحث :يهدف البحث الى الوصول الى مجموعة من الاهداف من أهمها التالي:

- توضيح العلاقة ما بين أمن المعلومات وثقة الزبون في شركات اسيا سيل، كورك تليكوم، نوروز.
- بيان تأثير أمن المعلومات على ثقة الزبون في الشركات المبحوثة.
- اعطاء اطار نظري لواحدة من اهم الحقول المستخدمة في مجال شركات الاتصالات والتي تتمثل بمتغيري أمن المعلومات وارتباطها بثقة الزبائن و اظهار امكانية استخدام تطبيقات وبرامجيات أمنة في شركات الاتصالات لغرض تحسين جودة الخدمات المقدمة من قبلها ولغرض الحصول على ثقة وولاء الزبائن بخدماتها على المدى البعيد.

1.4 فرضيات البحث

يسعى البحث الحالي الى اختبار الفرضيات الآتية :

الفرضية الأولى:

Ho: لا توجد علاقة ارتباط ذات تأثير معنوي ما بين أمن المعلومات وثقة الزبون

H1: توجد علاقة ارتباط ذات تأثير معنوي ما بين أمن المعلومات وثقة الزبون

الفرضية الثانية:

Ho: لا يوجد تأثير ذو دلالة معنوية لأمن المعلومات على ثقة الزبون.

H1: يوجد تأثير ذو دلالة معنوية لأمن المعلومات على ثقة الزبون.

1.5 حدود البحث

حدود البحث يمكن توضيحها من خلال التالي:

- الحدود الزمانية:بدأت الدراسة في كانون الاول 2017 وانتهت في ايار 2018 .
- الحدود المكانية: تضمنت شركات اسيا سيل ، كورك تليكوم، ونوروز في اربيل وبالتحديد اقسام تكنولوجيا المعلومات فيها.
- الحدود البشرية : تضمنت عينة من المتخصصين في اقسام تكنولوجيا المعلومات في الشركات الثلاث.

المحور الثاني: الجانب النظري

2.1 مفهوم أمن المعلومات

تتكون المعلومات من بتات من البيانات (الاصفار والواحدات)، ويمكن ان تنشأ نسخ طبق الاصل من المعلومات نتيجة قلة او عدم المتابعة للأنشطة، ويمكن ان يتم تعديل المعلومات بسهولة من خلال تغيير تفاصيل البيانات، ونظراً لطبيعة المعلومات المعقدة والمتداخلة فإنه لا يوجد طريقة لضمان حمايتها وأمنها بشكل كلي، ويقوم أمن المعلومات بمحاولة موازنة المخاطر في مواجهة كافة التحديات التي تواجهها المنظمة (Goss, 2009: 19). وفي الوقت الحالي تعتبر المعلومات

سلعة قيمة، ولذلك فهي بحاجة الى حماية، اذ ان المعلومات تؤثر على كافة جوانب منظمات الأعمال اليوم من الادارة العليا نزولاً الى مستوى الادارة التشغيلية. (Van Niekerk, 2010:1) ولغرض انجاح أمن المعلومات فإنه من الضروري الحصول على دعم الادارة العليا و تطبيق سياسات أمنية جيدة لغرض تقدير مستوى الخطر وتدريب الموظفين لزيادة الحماية، فضلاً ع تدقيق مدى التعرض للاختراقات و التصميم الجيد للشفرات المستخدمة. (Gregg et.al,2006:19). ان أمن المعلومات هو مصطلح يصف الحاجة لحماية المعلومات بناءً على حقيقة ان المعلومات مصنفة كأحد الموجودات القيمة. (Pettersson,2008:9).

وقد عرفت اللجنة الامريكية لأمن النظم القومية أمن المعلومات على انه " يتضمن حماية المعلومات (النظم) من الدخول الغير المخول، أو القيام بتعديل المعلومات، سواء كانت مخزنة ، معالجة ، او منقولة فضلاً عن الحماية من " الحرمان من الخدمة " Denial of Service " بالنسبة للمستخدمين المخولين للدخول لانظمة معينة، (Zegres, 2006 : 16). وتهدف هجمات " الحرمان من الخدمة " الى قطع الاتصالات مابين نقطتين ترتبطان بشكل لاسلكي، حيث تمنع هذه الهجمات طرفين مرتبطين بشكل شرعي من انشاء قناة اتصال آمنة (Pathan,2011:6).

ومنذ بداية الالفية الجديدة تطورت هجمات الحرمان من الخدمة من ازعاجات بسيطة الى تهديدات حقيقية وكبيرة للتجارة الالكترونية وكافة اشكال تطبيقات الشراء الالكتروني (Mclure 650 : 2009 , et.al). اذ أمن المعلومات هي حماية المعلومات وتفاصيلها الحساسة من أي مؤثوات خارجية، اذ تتضمن النظم والمكونات المادية، التي تستخدم لخرن ونقل المعلومات، و المفاهيم الاساسية لحماية موجودات المعلومات، والنظم المرتبطة بها من الاحداث الأمنية الخاصة بتقانة المعلومات (Puangsri,2001: 17).

يقوم أمن المعلومات بحماية المعلومات من مدى واسع من التهديدات وتقليل الاضرار التي تقلل من ارباح المنظمة من خلال التأثير على ثقة الزبون، فضلاً عن زيادة العائد على الاستثمار، اذ ان المعلومات تعد رأس مال مهم وحيوي يحتاج الى توفير الحماية الكافية (Soderbom 2007 : 10) ، بالاضافة الى ماسبق يقع على عاتق أمن المعلومات ايضاً حماية نظم المعلومات من الدخول غير المخول. (Van Opstal,2008:11). وقد قدمت (ISO) الوثيقة الاصل لـ (ISO7498/2) والتي عُرف من خلالها أمن المعلومات من خلال خمسة خدمات، اذ تعتبر (ISO7498/2) من افضل اطر العمل المرجعية التي تم تقديم أمن المعلومات من خلالها، والخدمات الخمسة التي حددتها ISO هي تحديد الهوية، المصادقة، التحويل، الموثوقية، التكاملية وعدم التنصل (Kritzinger, 2006 :9)، و اشارت مؤسسة SANS الى ان أمن المعلومات هو نتيجة لسياسات و/او اجراءات نظام معين للتحديد والمراقبة والحماية من الاختراق الغير المخول للمعلومات التي يتم اعطاء تخويل حمايتها من قبل السلطات التنفيذية او تشريعات القوانين (Goh, 2003 :20).

ذكرت مؤسسة SANS (Sysadmin, Audit, Network, Security) أن أمن المعلومات يتضمن العمليات والمنهجيات المراد منها حماية المعلومات والبيانات الحساسة من الدخول غير المخول اليها، او اختراقها ،او تعديلها ،او استخدامها، اذ ان المعلومات المحمية يمكن ان تكون الكترونية او (Putri & Mganga, 2011: 16). ويمكن تحديد مفهوم أمن المعلومات على انه المعيار المتبنى لمنع الاستخدام غير المخول اواساءة الاستخدام او التعديل والحرمان من استخدام المعرفة والحقائق و البيانات (Maiwald,2003:4). في حين عرف معيار ISO/IEC 17799 (المعيار العالمي لأمن تقانة المعلومات والمعروف بـ " تقانة المعلومات - الشفرة التنفيذية لادارة أمن المعلومات ") من خلال ثلاث مصطلحات " السرية " و " الدقة " و " قابلية الوصول " (Wallin & Xu,2008: 4).

2.2 متطلبات أمن المعلومات

ان اهم متطلب من متطلبات أمن المعلومات يتمثل بتوفير سياسة أمن معلومات مناسبة، و المنظمة التي ترغب بالحصول على سياسة أمن معلومات جيدة يجب ان تمتلك برنامج أمني يتضمن العديد من الخصائص التي تميزه وتعطيه القدرة على الحماية الكاملة من دون تدخل المستخدمين (Zegers, 2006: 29). بينما اكد (Nakrem,2007: 51) الى ان متطلبات أمن المعلومات تتمثل بالاتي:

- تقدير الخطر والتعامل معه: اي القيام بتحليل لمخاطر أمن المعلومات للمنظمة.
- السياسة الأمنية: اي توجيه الادارة ومستوى الأمن.
- تنظيم أمن المعلومات: اي القيام بحوكمة أمن المعلومات.
- ادارة الموجودات (الاصول): اي اجراء جرد والقيام بتصنيف موجودات المعلومات.
- امن الموارد البشرية: اي الجوانب الأمنية المتعلقة بدخول وتحرك ومغادرة الموظفين للمنظمة.
- الأمن المادي والبيئي: اي حماية المعدات الحاسوبية .
- ادارة العمليات والاتصالات: ادارة السيطرة على الأمن التقاني في النظم والشبكات.
- الرقابة على الدخول: اي تحديد حقوق الوصول للشبكات والنظم والتطبيقات والوظائف والبيانات.
- امتلاك نظم المعلومات والقيام بتطويرها وصيانتها: اي بناء الأمن ليصبح جزءا من التطبيقات.
- ادارة الاحداث العرضية لأمن المعلومات: توقع اختراقات أمن المعلومات، والاستجابة لها بشكل مناسب.
- ادارة استمرارية الاعمال: اي حماية، وادامة (صيانة) واصلاح النظم وعمليات الاعمال الحرجة.
- المسaire (المطاوعة): اي ضمان التوافق مع سياسة أمن المعلومات والمعايير والتشريعات والقوانين.

2.3 أهمية أمن المعلومات

يتم التشديد على أهمية أمن المعلومات بشكل اكبر في العالم يوماً بعد يوم، وذلك لان عمليات المعلومات تتداخل مع العمليات والتعاملات اليومية، ومن ضمنها ادارة الاعمال ، والتعليم، والصحة، وجوانب اخرى من الحياة اليومية (Kizza & Kizza, 2008: 49).

أ- **الأمن المالي:** تشير المعلومات المالية الى المعلومات ذات القيمة المالية، وبسبب هذه القيمة فان هذه المعلومات تحتاج للحماية، و يشير الأمن المالي الى الاساليب التي يتم من خلالها حماية المعلومات ذات العلاقة باموال الافراد.

ب- **أمن الحاسوب:** تقوم الحواسيب بتخزين كميات هائلة من المعلومات الشخصية الخاصة بالصحة والاموال والتعليم وادارة الاعمال وكل مايقع في متضمناتها، اذ أن المعلومات قيمة لذا يجب حمايتها، و هذه القيمة الي يتم تخزينها في الحواسيب جعلت هذه الحواسيب عرضة للسرقة والتخريب.

ت- **أمن الشبكات:** مع زيادة ارتباط الحواسيب مع بعضها البعض، ظهرت شبكات موزعة للحواسيب، اذ بدأ مصطلح أمن الحواسيب يعطي طريق لمصطلح جديد والذي هو " أمن الشبكات"، حيث توسعت المتطلبات الان لتشمل الرقابة على الدخول لنقاط الوصول للشبكة مثل الموجهات، والخوادم، وكذلك الرقابة على الوصول للحواسيب المفردة من اجل تقليل الخطر، وتكون الشبكات آمنة اذا ما استطعنا الرقابة على الوصول الى كافة نقاط الوصول للشبكة، والتي يمكن توضيحها من خلال الاتي: (Ciampa, 2009: 13)

- **منع سرقة البيانات:** ان منع سرقة المعلومات تعد من الاهداف الاساسية لأمن المعلومات من قبل مؤسسات الاعمال، حيث ان سرقة بيانات الاعمال تتضمن سرقة معلومات مثل، قائمة بالزبائن الذين يرغب المنافسين في الحصول عليهم.

- **سرقة الهويات الشخصية:** ان سرقة الهوية تتضمن سرقة المعلومات الشخصية الخاصة باحدهم، مثل سرقة رقم الأمن الاجتماعي لانشاء حسابات بطاقات ائتمان، وانشاء حسابات المصارف والتي تترك فيما بعد بدون دفع.

- **تجنب التبعات القانونية:** في السنوات الماضية ظهرت العديد من القوانين التي كان الهدف منها حماية خصوصية البيانات الالكترونية، اذ ان مؤسسات الاعمال التي تفشل في حماية بياناتها ربما تواجه العديد من التبعات القانونية .

2.4 تصنيفات أمن المعلومات

اشار (Nampana, 2012: 19) الى انه يمكن تقسيم المعلومات الى ثلاث تصنيفات اساسية يمكن ان تستخدم في العديد من المنظمات وكما يلي:

1- **موثوقة:** يستخدم هذا التصنيف لأكثر المعلومات المشتركة حساسية، ويتم الرقابة المشددة عليها من قبل المنظمة، والوصول اليها مبني على اساس ما تحتاج الوصول اليه، او حسب ما تتضمنه بنود العقد.

2- **داخلية:** يستخدم هذا التصنيف مع المعلومات الداخلية، والتي لا تتوافق مع معايير تصنيف المعلومات الموثوقة السابقة، ويمكن الدخول اليها واستعراضها فقط من قبل موظفي الشركة والمقاولين المخولين واطراف اخرى.

3- **خارجية:** تشمل كل المعلومات والتي تم الموافقة عليها من قبل الادارة للاستخدام العام .
بينما اكد (Bellefeuille,2005:20) الى انه يمكن ان يتم تصنيف أمن المعلومات بشكل تفصيلي الى الاحداث والهجمات والاحداث العرضية والتي سنوضحها بشكل تفصيلي كما يلي:

- **الاحداث:** بالاخذ بنظر الاعتبار ان الاحداث العرضية تنشأ عادة من الاحداث والتي تتكون من هجمة واحدة او مجموعة من الهجمات، فانه يمكن فهم الحادث العرضي من خلال دراسة اكثر مكوناتها الاساسية وهو الحدث، حيث يعرف الحدث على انه اجراء متخذ للوصول الى هدف، والذي ينتج عن تغيير الحالة او الوضع الحالي للنظام او الاداة المستهدفة.بينما اشار (Koivunen,2010:4) الى انه يمكن تعريف الحدث حسب مؤسسة (IEEE) على انه " اجراء يوجه لتنفيذه على هدف معين المراد منه الحصول على نتيجة تغير من الحالة او الوضع الحالي للهدف.

- **الهجمات:** يتم تنفيذ الهجمات من خلال سلسلة من الخطوات المجتمعة من قبل المهاجم لادراك نتائج معينة بطريقة غير مخولة، يتم وضع خصائص للهجمات من خلال تجميع مجموعة خطوات منطقية يتخذها المهاجم، و يستخدم المهاجم اداة معينة لاستغلال نقطة ضعف معينة، حيث تقوم الاداة باتخاذ اجراء معين في مواجهة الجهة المستهدفة.

- **الاحداث العرضية:** ان الاحداث العرضية هي سياق معين متعلق بهجوم معين، اذ يُسمح بتجميعها مع هجمات اخرى بناءً على نوعية الهجمات التي تم تنفيذها، حيث ان المكان والوقت للهجمة يشار اليه عادة بالحادث العرضي، ويمكن تمييز الحادث العرضي من خلال نوع المهاجم وهدفه، اذ ان معرفة نوع المهاجم تعتبر جزء مهم لتحديد دوافعه واهدافه التالية.

2.5 معايير أمن المعلومات

تسعى المعايير الأمنية الى توفير الحد الأدنى من القواعد الالزامية التي ينبغي على المنظمات الالتزام بها من اجل توفير المستويات الأمنية المرضية، ويمكن تعريف المعيار الى انه " الانشطة والقواعد والاجراءات الالزامية"، والمعايير يمكن ان تكون داخلية او خارجية (مثل القوانين والتشريعات الحكومية). (Harris,2008:112) ، وفيما يلي تعداد لأهم هذه المعايير:

▪ **معيار مباديء أمن النظم المقبولة بشكل عام (GASSP):** وقد تم نشره من قبل الابحاث القومية للولايات المتحدة الامريكية وهو يتضمن اربع اهداف، الوصول الى التنفيذ الجيد لأمن

المعلومات، بناء نقطة مرجعية ومرجعية قانونية لمبادئ وآراء وممارسات الأمن، والتحسين المستمر لكفاءة وفعالية وظائف أمن تقانة المعلومات، امتلاك بنية معرفية قادرة على التحقق من أمن المعلومات (Al-Azazi 2008:49).

▪ **معيار ISO/IEC 27001** :ويعد من اهم معايير **IEC:ISO** يحدد هذا المعيار متطلبات انشاء، تنفيذ، تشغيل ومراقبة ومراجعة وإدامة وتحسين نظم ادارة أمن المعلومات الموثقة. (Nakrem , 2007:16).

▪ **معيار التنفيذ الجيد لأمن المعلومات** : يتناول هذا المعيار أمن المعلومات من وجهة نظر الاعمال من اجل تقدير استعدادات المنظمة لتنفيذ أمن المعلومات، حيث انها تركز على الاستعدادات الخاصة بالمنظمة لجعل مخاطر الاعمال ذات العلاقة بنظم المعلومات الحساسة تحت السيطرة ضمن البيئة التنافسية والديناميكية المتواجدة اليوم (Zegers, 2006:35).

▪ **معيار 2005: ISO 27002**: وهو معيار اخر من معايير ISO الخاصة بأمن المعلومات وتقانات الأمن - الشفرة التنفيذية، والذي يتكون من افضل الممارسات العالمية لحماية النظم. (Jackson, 2010:77).

▪ **معيار Gramm-Leach-Bliley Act**: وهو يعد من اهم المعايير التي غزت بها الحكومة الامريكية مجال معايير أمن المعلومات مما تطلب انشاء وسائل الوقاية المناسبة التي تتضمن، التأكد من موثوقية وأمن سجلات ومعلومات الزبائن، الحماية من التهديدات والمخاطر (Cunningham et.al, 2007: 289).

▪ **المعيار البريطاني BS 7799**: تم نشره في بريطانيا عام 1995 والهدف منه السماح للشركات التي تخضع لهذا المعيار باظهار قدرتها على التأكيد على عدم قدرة انتهاك الموثوقية والتكاملية والتوافرية للبيانات باي طريقة من الطرق (Kritzinger, 2006:46).

▪ **معيار معالجة المعلومات الفيدرالية FIPS 140-2**: وهو معيار يصف متطلبات تشفير البيانات الغير المصنفة وقد تم نشره من قبل المؤسسة القومية للمعايير والتكنولوجيا (NIST) وتم اعتماده بعد ذلك كاحد المعايير الفعلية، ويعرف هذا المعيار المستويات الأمنية الى المستوى الاول الاقل الى المستوى الرابع. (Osborne, 2006:102).

2.6 مفهوم الثقة

الثقة تمثل الاعتقاد الذي يجعل زبون معين مرتبطاً بمنظمة معينة، وقد تتضمن الثقة ايضا الثقة التي تسود ما بين الموظفين في المنظمة، اذ تعد الثقة عامل مهم جداً لبناء الولاء عند الزبون من خلال توفير المنتجات والخدمات التي ترضي الزبائن. (Sarwar, et.al, 2012: 26- 36).

وكما اشار (Lee, 2005 : 169) ان الثقة تمثل مقياس مهم لمكانة المنظمة في السوق نظراً لكون الثقة توفر نسبة توقع عالية للصفقات الناجحة، فضلاً عن كون الثقة عامل مهم في التأثير على سلوك الزبون والذي يمثل عامل ايجابي مهم في بيئات عدم التأكد والثقة تمثل عامل مهم لدى الزبون

لتقبل التقانات الحديثة خصوصاً تطبيقات الانترنت. من جهة أخرى يمكن القول ان الثقة تمثل العلاقة الوثيقة ما بين قيمة الثقة والسلوكيات التي تنتج عن هذه الثقة والتي تصب في مصلحة المنظمة من جهة والزبون من جهة ثانية. (17 : 2002 , Sirdeshmukh *et al.*) والثقة تمثل واحدة من المقاييس التي تحدد العلاقة ما بين الجودة، والتي من المعتقد انها تزيد من شعور الامان لدى الزبون وتقلل من مستويات عدم التأكد لديه، وبالتالي تساهم في بناء بيئة داعمة لكافة الاطراف سواء الزبون او المنظمة (Balla *et al.*, 2015: 4). من جانب آخر تمثل الثقة النية الكاملة للاعتماد على اطراف اخرى في مرحلة الخطر وهذا يأتي من الفهم الكامل للطرف الآخر والذي يكون مبنياً على خبرات سابقة (Upamannyu *et al.*, 2015: 4). بينما اوضح (Nguyen, 2013: 99) ان الثقة تمثل مستوى الاعتمادية والذي يقدم من قبل طرف معين الى الطرف الآخر على اساس العلاقة التبادلية التي تربط بينهما.

2.7 مداخل دراسة ثقة الزبون

يمكن دراسة ثقة الزبون من خلال العديد من الاساليب والمداخل التي يمكن توضيحها من خلال الآتي:

(Chinomona, *et al.*, 2014: 25)

- المدخل الأول لدراسة الثقة يمثل اعتقاد او توقع مسبق عن طرف آخر الذي يعتمد على خبرات سابقة للتعامل مع هذا الطرف واعتمادية كاملة مبنية ايضاً على خبرات سابقة.
- المدخل الآخر اظهر الثقة على انها اعتماد طرف معين على طرف آخر بسبب امكانية تعرضهم للأخطار او عدم التأكد الذي يكون في بيئة المنظمة.

2.8 اهمية ثقة الزبون

تعد الثقة عاملاً مهماً في العلاقة ما بين الالتزام وولاء الزبون فاذا امتلك طرف معين ثقة كاملة بالطرف الآخر، فلا بد للطرف الاخر ان يكون على قدر هذه الثقة من خلال المحاولة الدائمة لترك اثر ايجابي لدى الطرف المقابل، فعندما يضع الزبون ثقته بمنظمة معينة فان هذا الزبون يسعى الى تقديم اسلوب شراء ايجابي تجاه المنظمة ، فعندما تقدم المنظمة خدماتها بأسلوب معين يعمل على بناء ثقة متبادلة مع الزبون، سيؤدي ذلك الى تقليل المخاطر التي تعترض تقديم هذه الخدمات وبالتالي تحقيق النجاح للمنظمة. (Vuuren *et al.*, 2012: 85).

2.9 خصائص الثقة

تمتلك الثقة ثلاث خصائص اساسية كمايلي: (Suh and Han, 2003: 137)

- **المقدرة:** تعني ان الشخص الذي يضع ثقته بالطرف الآخر يعتقد ان الطرف الاخر لديه القابلية او القوة الكافية التي تمكنه من القيام بمايلزم وقت الحاجة.
- **النية الطيبة:** تعني المدى الذي يعتقد ان الشخص الموثوق يرغب بالقيام بتصرفات جيدة تجاه الطرف الآخر، بعيداً عن اي اسباب ربحية اخرى.

- **التكاملية:** المدى الذي يجعل الشخص الموثوق يوافق على اتفاقات معينة، والايفاء بكل الوعود التي قطعها بشكل كامل.

2.10 تقنيات ثقة الزبون في الانترنت

هنالك العديد من التقنيات المستخدمة للحصول على ثقة الزبون من خلال المنظمات التي تعتمد الانترنت وتطبيقاته والتي يمكن توضيحها من خلال الآتي: (Gustavsson & Johansson, 2006: 26)

- **التسويق:** لغرض تكوين بيئة موثوقة مابين الاطراف المختلفة كان لابد من استخدام التسويق كاسلوب مهم للحصول على ثقة الزبون، وبناءً على ذلك يوفر التسويق للمنظمة الفرصة المناسبة للزبون للتفاعل مع موقع الانترنت بشكل قانوني وواضح.
- **الشفافية:** تعتبر افضل طريقة لتجنب اضرار الثقة، تتمثل بالوضوح في المعلومات المتداولة وذلك لغرض الوصول الى مستوى صدق معين عن اي وضع او ظرف معين يمكن ان تواجهه المنظمة.
- **الحماية:** تمثل نوع معين من الثقة التي يمكن انشاءها من خلال المساعدة في حماية البرامج، وهذه وهذه البرامج تقدم شبكات حماية، لكل الاعضاء لغرض ايجاد حلول في حالة كل حدوث اي خطأ.
- **التشفير:** تعتبر وسيلة قوية لبناء الثقة والتي تتبع من تشفير موقع معين ، وبما ان الشفرة الحقيقية لاتكون واضحة للمستخدمين فان هذا يؤدي الى الاعتماد على عناصر اكثر وضوحاً، (على سبيل المثال جودة تصميم واجهة المستخدم، السرعة وغيرها.

المحور الثالث / الجانب العملي

3.1 نبذة مختصرة عن شركات أسيا سيل وكورك ونوروز (مجال التطبيق)

تعتبر شركة اسيا سيل من اهم مجهزي خدمات الاتصالات وخدمات البيانات في العراق اذ بلغت قاعدة مستخدميها في العراق مايقارب 12,5 مليون مشترك في كانون الثاني 2017، وقد كانت اسيا سيل الشركة الاولى في العراق التي توفر خدمة الاتصال الدولي، والتي توفر خدماتها الى 18 محافظة عراقية بضمنها العاصمة بغداد. بينما تعتبر كورك تيليكوم من الشركات المهمة في تجهيز خدمة الاتصالات، حيث تغطي القطر بالكامل وتوفر تقنياتها المتطورة افضل الخدمات وباعلى المستويات، وتخدم هذه الشركة في 18 محافظة عراقية من خلال تقديمها لاتصالات لاسلكية والتي تعطي حرية التنقل للمستخدمين، من خلال توفير خدمات GSM وتعتبر شركة كورك متميزة عن غيرها من خلال تقديمها لافضل الخدمات وباعلى جودة وبافضل الاسعار. وتعد نوروز تيليكوم هي شركة خاصة تأسست عام 2007، باعتبارها مزوداً رائداً لمجموعة واسعة من خدمات الاتصالات السلكية واللاسلكية للاتصالات الصوتية والبيانات في إقليم كردستان العراق. آلاي نوروز تيليكوم

تمتلك الرؤية المستقبلية لبناء أحدث اللنى التحتية والهياكل الأساسية للاتصالات من أجل تسهيل حياة عملائها وتقدم مجموعة واسعة من خدمات نقل البيانات خلافاً لمنافسيها.

3.2 وصف مجال تطبيق البحث: تضمنت عينة الدراسة مجموعة من الموظفين العاملين في مجال تكنولوجيا المعلومات في شركات نوروز تيليكون وشركة كورك تيليكون وشركة اسياسيل في مدينة اربيل وكان عدد الاستثمارات الموزعة على الشركات الثلاث بشكل عام (61) استثماراً ، اذ بلغ عدد الاستثمارات الموزعة في شركة كورك 32 استثماراً في حين تم توزيع 10 استثمارات في شركة نوروز و 19 استثماراً في شركة اسياسيل ، اذ تم توزيع الاستثمارات بشكل عام على كافة الموظفين العاملين في اقسام تكنولوجيا المعلومات.

3.3 التكرارات والنسب المئوية لأجابات عينة البحث لمتغير أمن المعلومات

تضمنت استمارة الاستبيان متغيرين رئيسيين الأول متغير أمن المعلومات ويعتبر المتغير المستقل في الدراسة والمتغير المعتمد والذي يمثل ثقة الزبون ويمكن توضيح التكرارات والنسب المئوية لأجابات عينة الدراسة للمتغير الأول أمن المعلومات من خلال الجدول الآتي:

الجدول (1)

التكرارات والنسب المئوية لأجابات عينة البحث لمتغير (أمن المعلومات)

ت	الاسئلة	معدل الاستجابة							
		موافق بشدة		موافق		محايد		غير موافق	
		النسب	التكرارات	النسب	التكرارات	النسب	التكرارات	النسب	التكرارات
1	توفر الشركة تدريب جيد يحدد ماهية المعلومات التي يجب الحفاظ عليها وإبقائها، والمعلومات التي تعد غير ضرورية ويمكن الاستغناء عنها.	54.1	33	32.8	20	4.9	3	6.6	4
2	تمتلك الشركة نسخ احتياطية عن أي معلومات يتم استبدالها أو تدميرها أو اوسرقتها ويتم حفظها بأشكال إلكترونية مختلفة.	31.1	19	50.8	31	13.1	8	3.3	2
3	هنالك دعم كامل من قبل الإدارة في المنظمة لرفع مستوى أمن المعلومات من خلال استخدام تدريب الموظفين وزيادة وعيهم والسياسات والإجراءات التي تخدم في هذا المجال.	29.5	18	36.1	22	14.75	9	4.9	3
4	تلعب الحوافز الملموسة مثل الترقيات والأموال والحوافز غير الملموسة مثل الرضا والتقدير دوراً كبيراً في التزام الأفراد في المنظمة بالسياسات الأمنية في المنظمة	32.8	20	45.9	28	16.4	10	1.6	1
5	تعتبر أنظمة كلمات المرور المستخدمة في المنظمة قوية وغير قابلة للاختراق (أي لا تتضمن أسماء أفراد، أرقام ضمان اجتماعي أو أية معلومات شخصية يسهل اختراقها)	32.8	20	32.8	20	26.2	16	3.3	2

6	يتم اتخاذ القرارات في المنظمة عادة على اساس وضع الاولوية للزبون ووضع المتطلبات الأمنية والتقنية لخدمة الزبون.	12	19.7	28	45.9	12	19.7	6	9.8	3	4.9
7	تمتلك المنظمة السياسات الأمنية الملائمة والتي تجعل المعلومات المنقولة بشكل الكتروني عبر انظمتها تتمتع بالموثوقية والتكاملية والتوافرية.	16	26.2	33	54.1	5	8.2	4	6.6	3	4.9
8	تحصل ادارة المنظمة على تقارير دورية تتضمن شرح لمستوى أمن المعلومات او اية اختراقات أمنية حال حدوثها.	14	23.0	31	50.8	7	11.5	6	9.8	3	4.9

تم تحليل اجابات الافراد المبحوثين من خلال استخدام برنامج SPSS اذ أظهرت نتائج التحليل الاحصائي لأجابات عينة البحث الى ان ما نسبته (54.1%) اتفقوا بشدة على ان الشركة توفر تدريب جيد يحدد ماهية المعلومات التي يجب الحفاظ عليها وابقائها والمعلومات التي تعد غير ضرورية ويمكن الاستغناء عنها من ناحية اخرى فأما نسبة (1.6%) كانوا غير متفقين بشدة مع ذلك. من ناحية اخرى فان ما نسبته ما نسبته (50.8%) كانت اجاباتهم متفقة على ان الشركة تمتلك الشركة نسخ احتياطية عن اية معلومات يتم استبدالها او تدميرها او اوسرقتها ويتم حفظها باشكل الالكتروني مختلفة، من جانب آخر فأما نسبته (1.6%) كانوا غير متفقين بشدة مع ذلك.

في حين ان اجابات عينة البحث بينت ان ما نسبته (36.1%) اتفقت اجاباتهم على ان هنالك دعم كامل من قبل الادارة في المنظمة لرفع مستوى أمن المعلومات من خلال استخدام تدريب الموظفين وزيادة وعيهم والسياسات والاجراءات التي تخدم في هذا المجال ، من جانب آخر فأما نسبته (4.9%) كانت اجاباتهم غير متفقة بشدة مع ذلك. و بينت اجابات المبحوثين ان ما نسبته (45.9%) اتفقت اجاباتهم على انه تلعب الحوافز الملموسة مثل الترقيات والاموال والحوافز غير الملموسة مثل الرضا والتقدير دوراً كبيراً في التزام الافراد في المنظمة بالسياسات الأمنية في المنظمة ، من جانب آخر فأما نسبته (1.6%) كانت اجاباتهم غير متفقة مع ذلك. فيما اظهرت نتائج التحليل أن ما نسبته (45.1%) اتفقت اجاباتهم على انه تعتبر انظمة كلمات المرور المستخدمة في المنظمة قوية وغير قابلة للاختراق (اي لا تتضمن اسماء افراد، ارقام ضمان اجتماعي او اية معلومات شخصية يسهل اختراقها)، في حين أن نسبة (3.3%) كانت اجاباتهم غير متفقة مع ذلك. بينما اتفقت اجابات (33.2%) على انه يتم اتخاذ القرارات في المنظمة عادة على اساس وضع الاولوية للزبون ووضع المتطلبات الأمنية والتقنية لخدمة الزبون ، في حين أن ما نسبته (4.9%) كانت اجاباتهم غير متفقة بشدة مع ذلك.

فيما تبين ان ما نسبته (54.1%) اتفقت اجاباتهم على انه تمتلك المنظمة السياسات الأمنية الملائمة والتي تجعل المعلومات المنقولة بشكل الكتروني عبر انظمتها تتمتع بالموثوقية والتكاملية والتوافرية، بينما كانت نسبة (4.9%) غير متفقة بشدة مع ذلك. فيما بينت اجابات المبحوثين ان ما نسبته

(50.8%) اتفقت اجاباتهم على انه تلعب الحوافز الملموسة مثل الترقيات والاموال والحوافز غير الملموسة مثل الرضا والتقدير دوراً كبيراً في التزام الافراد في المنظمة بالسياسات الأمنية في المنظمة ، من جانب آخر فأن مانسبته (4.9%) كانت اجاباتهم غير متفقة بشدة مع ذلك.

3.5 التكرارات والنسب المئوية للمتغير المعتمد (ثقة الزبون)

الجدول (2)

التكرارات والنسب المئوية لأجابات عينة البحث لمتغير (ثقة الزبون)

ت	معدل الاستجابة	معدل الاستجابة							
		موافق بشدة		موافق		محايد		غير موافق	
		النسب	التكرار	النسب	التكرار	النسب	التكرار	النسب	التكرار
		النسب المئوية	ارات	النسب المئوية	ارات	النسب المئوية	ارات	النسب المئوية	ارات
1	الشركة تبذل أقصى ما بوسعها لتقديم افضل الخدمات التي ترضي حاجات زبائننا.	42.6	26	36.1	22	18.0	11	1.65	1
2	الشركة تمتلك سمعة جيدة بسبب تعاملها الجيد مع زبائننا.	36.1	22	47.5	29	11.5	7	3.3	2
3	الشركة تستطلع اراء زبائننا بشكل دوري عن مستوى الخدمات المقدمة من خلال استمارات استبيان دورية .	14.8	9	52.8	32	23.0	14	8.2	5
4	الشركة توفر خدمات الانترنت المتنقلة لكافة زبائننا.	18.0	11	57.4	35	18.0	11	3.3	2
5	ادارة الشركة تتعامل مع جميع العاملين والزبائن بصدق ونزاهة ، وتحاول ايفاء جميع وعودها المقدمة للزبائن.	21.3	13	49.2	30	21.3	13	4.1	2
6	سهولة الموقع الالكتروني تجعله قادر على مساعدة الزبائن على ايجاد الخدمات التي يريدونها بسهولة.	23	14	49.2	30	16.4	10	5.75	3
7	ادارة الشركة تهدف الى زيادة القدرات والمهارات الفردية والجماعية للعاملين.	36.1	22	34.4	21	26.2	16	1.65	1
8	قيادة الشركة تسعى دوماً الى التنمية الذاتية لقدرات العمل في مجالات العمل المختلفة.	18.0	11	39.3	24	34.4	21	6.6	4
9	الشركة توظف العلاقات غير الرسمية مع زبائننا لغرض الحصول على ثقة الزبون الكاملة في مجالات العمل.	21.3	13	42.6	26	23.0	14	8.2	5
10	اسلوب عمل الشركة ومعرفتها بدقائق الأمور يساهم بشكل كبير في رفع مستوى ثقة زبائننا بالخدمات التي تقدمها.	24.6	15	42.6	26	16.4	10	9.8	6
11	تسعى ادارة الشركة لزيادة القدرات والمهارات الفردية والتقانية للعاملين، مما يؤثر ايجابياً في المستقبل في الحصول على ثقة الزبون.	26.2	16	42.6	26	18.0	11	3.3	2

بينت اجابات عينة البحث ان (42.6%) اتفقت اجاباتهم بشدة على ان الشركة تبذل اقصى ماوسعها لتقديم افضل الخدمات التي ترضي حاجات الزبائن، من جانب آخر فإن (1.65%) كانت اجاباتهم غير متفقة بشدة مع ذلك. بينما كانت نسبة (47.5%) اتفقت اجاباتهم على ان الشركة تمتلك سمعة جيدة بسبب تعاملها الجيد مع زبائنهم، في حين أن (1.6%) كانت اجاباتهم غير متفقة بشدة مع ذلك. من جانب آخر تبين أن (52.8%) اتفقت اجاباتهم على ان الشركة تستطلع اراء زبائنهم بشكل دوري عن مستوى الخدمات المقدمة للزبائن من خلال استمارات استبيان دورية ، و نسبة (1.6%) كانت اجاباتهم غير متفقة بشدة مع ذلك. فيما بينت اجابات المبحوثين ان مانسبته (57.4%) اتفقت اجاباتهم على انه الشركة توفر خدمات الانترنت المتنقلة لكافة زبائنهم.، من جانب آخر فإن مانسبته (3.3%) كانت اجاباتهم غير متفقة بشدة مع ذلك.

في حين اتفقت اجابات (49.2%) على ان ادارة الشركة تتعامل مع جميع العاملين والزبائن بصدق ونزاهة ، وتحاول ايفاء جميع وعودها المقدمة للزبائن، بينما كانت نسبة (4.1%) غير متفقين بشدة مع ذلك. وقد لوحظ ان مانسبته (49.2%) اتفقت ان سهولة الموقع الالكتروني تجعله قادر على مساعدة الزبائن على ايجاد الخدمات التي يريدونها بسهولة، من جانب آخر فإن مانسبته (5.75%) كانت اجاباتهم غير متفقة بشدة مع ذلك. بينما تبين أن نسبة (36.1%) اتفقت اجاباتهم بشدة على ان ادارة الشركة تهدف الى زيادة القدرات والمهارات الفردية والجماعية للعاملين، في حين أن نسبة (1.65%) كانت اجاباتهم غير متفقة بشدة مع ذلك. بينما اتفقت نسبة (39.3%) على انه قيادة الشركة تسعى دوماً الى التنمية الذاتية لقدرات العمل في مجالات العمل المختلفة ، في حين أن نسبة (1.6%) كانت اجاباتهم غير متفقة بشدة مع ذلك.

بينما اتفق (42.6%) على أن الشركة توظف العلاقات غير الرسمية مع زبائنهم لغرض الحصول على ثقة الزبون الكاملة في مجالات العمل، في حين كان (4.9%) غير متفقين بشدة مع ذلك. فيما بينت اجابات المبحوثين ان مانسبته (42.6%) اتفقت اجاباتهم على ان اسلوب عمل الشركة ومعرفتها بدقائق الأمور يساهم بشكل كبير في رفع مستوى ثقة زبائنهم بالخدمات التي تقدمها، من جانب آخر فإن مانسبته (6.6%) كانت اجاباتهم غير متفقة مع ذلك. في حين اتفق (42.6%) على انه تسعى ادارة الشركة لزيادة القدرات والمهارات الفردية والتقانية للعاملين، مما يؤثر ايجابياً في المستقبل للحصول على ثقة الزبون، في حين أن (3.3%) كانت اجاباتهم غير متفقة مع ذلك.

3.6 اختبار فرضيات البحث: تركزت فرضيات البحث على قياس العلاقة والتأثير ما بين متغيري البحث، وتم ذلك من خلال استخدام الآتي:

3.6.1 الارتباط: تم استخدام اختبار بيرسون لقياس مدى الارتباط ما بين متغيري البحث وكما هو موضح في الجدول الآتي:

الجدول (3)

ارتباط بيرسون مابين أمن المعلومات وثقة الزبون

	أمن المعلومات	ثقة الزبون
Pearson Correlation	1	.516**
Sig. (2-tailed)		.000
N	61	61
Pearson Correlation	.516**	1
Sig. (2-tailed)	.000	
N	61	61

**. Correlation is significant at the 0.01 level (2-tailed).

وبالاعتماد على فرضيات البحث فان نتائج التحليل الاحصائي التي تم الحصول عليها من برنامج SPSS اظهرت ان قيمة P بلغت (0.000) وهي اقل من ($\alpha = 0.05$) ، سنرفض فرضية العدم ونقبل الفرضية البديلة مما يعني انه توجد علاقة ارتباط طردية متوسطة القوة مابين متغيري أمن المعلومات وثقة الزبون ، اذا بلغت قيمة ارتباط بيرسون 0.51% عند مستوى معنوية (0.000) والذي يعني وجود علاقة ارتباط ذات دلالة معنوية مابين متغيرات البحث.

3.6.2 الانحدار

تم استخدام معامل الانحدار الخطي البسيط مابين متغيري البحث (أمن المعلومات، وثقة الزبون) والذي يتضمن تحليل Anova الضروري لحساب مدى معنوية وتأثير المتغير المستقل (أمن المعلومات) على المتغير المعتمد (ثقة الزبون).

الجدول (4)

الانحدار الخطي البسيط

Model	Sum of Squares	Df	Mean Square	F	Sig.
1 Regression	4.033	1	4.033	21.376	.000 ^a
Residual	11.131	59	.189		
Total	15.163	60			

تضمنت الفرضية الرئيسية الثانية قياس مدى تأثير متغير أمن المعلومات على متغير ثقة الزبون، وبما أن نتائج التحليل الاحصائي التي تم الحصول عليها من برنامج SPSS اظهرت ان قيمة P بلغت (0.000) وهي اقل من ($\alpha = 0.05$) ، سنرفض فرضية العدم ونقبل الفرضية البديلة مما يعني انه يوجد تأثير ذو دلالة معنوية مابين متغيري أمن المعلومات وثقة الزبون.

المحور الرابع / الاستنتاجات والتوصيات

4.1 الاستنتاجات

- 1- تبين ان الشركات المبحوثة تمتلك السياسات الأمنية الملائمة والتي تجعل المعلومات المنقولة بشكل الكتروني عبر انظمتها تتمتع بالموثوقية والتكاملية والتوافرية.
- 2- أمن المعلومات يتضمن توفير الحماية الكافية للمعلومات وعناصرها الحساسة والمتضمنة النظم والمكونات المادية، التي تستخدم لخرن ونقل المعلومات.
- 3- ثقة الزبون تعد من اساسيات بقاء الزبون واستمراره في التعامل مع الشركة، والتي تتبع من رضاه الدائم عن الخدمات التي يحصل عليها، اذ تبين ان ادارة الشركات المبحوثة تتعامل مع جميع العاملين والزبائن بصدق ونزاهة، وتحاول ايفاء جميع وعودها المقدمة للزبائن.
- 4- توجد علاقة ارتباط طردية ومعنوية ما بين متغيري أمن المعلومات و ثقة الزبون مما يدل على اهمية الاهتمام بهذين العاملين داخل المنظمة سوياً .
- 5- يوجد تأثير معنوي لأمن المعلومات على ثقة الزبون فكلما زاد مستوى أمان المعلومات المنقولة كلما ادى ذلك الى زيادة ثقة الزبون اكثر بالتعامل مع شركات الاتصال خصوصاً في العصر الحالي الذي تكثر فيه حالات القرصنة .

4.2 التوصيات

- 1- زيادة الوعي باهمية استخدام التقانات الحديثة للحفاظ على أمن المعلومات كاستخدام معدات شركة سيسكو التي تعد الاقوى في مجال حماية المعلومات الأمر الذي يساهم في رفع مستوى ثقة الزبون .
- 2- اهمية اعطاء الزبون الخصوصية الكافية من خلال استخدام انظمة ادارة ذاتية لخدمات الانترنت من دون اطلاع شركات الاتصالات على محتوى المعلومات والبيانات المنقولة من والى الزبون.
- 3- ضرورة استخدام الشركات لشبكات داخلية تغنيها عن استخدام الانترنت العام والذي قد يتعرض للقطع في حال حدوث اي مشاكل داخلية او خارجية بالاضافة الى استخدام تقنية الشبكة الافتراضية الخاصة التي تجعل عملية نقل البيانات الشخصية تتم بشكل سري وآمن.
- 4- تعد ثقة الزبون من اهم محركات الحصول على الميزة التنافسية خصوصاً ما بين شركات الاتصالات التي تتمتع بالمنافسة الشديدة في خدمات الاتصالات وخدمات الانترنت على حد سواء.

المصادر

- 1- Al-Azazi, Sabri(2008), A multi-layer model for e-government information security assessment, Phd Thesis, School Of Applied Sciences, Cranfield University.
- 2- Bellefeuille, Cynthia, (2005), quantifying the and managing the risks of information security breaches to the supply chain, master thesis, engineering systems division, Massachusetts institute of technology.

- 3- Chinomona , Richard & Dubihlela Dorah, 2014, Does Customer Satisfaction Lead to Customer Trust, Loyalty and Repurchase Intention of Local Store Brands? The Case of Gauteng Province of South Africa, Mediterranean Journal of Social Sciences, Vol 5, No 9, MCSER Publishing, Rome-Italy, (pp. 23-32).
- 4- Ciampa, Mark, (2009), Security + Guide to Network Security Fundamentals, 3rd Edition, Course Technology, Cengage Learning, Nelson Education, Ltd, Canada.
- 5- Cunningham, Bryan & Manzuik, Steve & Dykstra, Greg & Miles, Ted Fuller, Ed C. & Morgan, Forrest & Gatford, Chris & Pfeil, Ken & Gold , André & Rogers, Russ & Hoagberg, Paul, Matthew & Schack, Travis & Hubbard, Amanda Snedaker , Susan & Little , Chuck, (2007), the best damn IT security management book period, Syngress Publishing, Inc., Elsevier, Inc.
- 6- Goh, Rita, (2003), Information Security: The Importance of the Human Element , Dissertation , Faculty of the Preston University, Singapore.
- 7- Goss, Ryan Gavin, (2009) , Enabling e-Learning 2.0 in Information Security Education : A Semantic Web Approach, dissertation, Faculty of Engineering, The Built Environment and Information Technology, Nelson Mandela Metropolitan University.
- 8- Gregg, Michael & Watkins, Stephen & Mays, George & Ries, Chris & Bandes, Ron & Franklin, Brandon, (2006) , Hack The Stack, Syngress Publishing, Inc., USA.
- 9- Gustavsson, Malin And Johansson, Ann-Marie, (2006), Consumer Trust In E-Commerce, Bachelor Thesis, Kristianstad University, pp. 23).
- 10- Jackson, Chris, (2010), network security auditing, CISCO press, cisco systems, Inc., USA.
- 11- Kizza, Joseph M. & Kizza, Florence M., (2008), Securing the Information Infrastructure, 2008 by IGI Global.
- 12- Koivunen, Erka (2010), effective information sharing for incident response coordination reporting network and Information Security Incidents and Requesting Assistance, Faculty of Electronics, Communications and Automation.
- 13- Kritzenger, Elmarie, (2006), An Information Security Retrieval And Awareness Model For Industry, Doctor Of Philosophy, University Of South Africa.
- 14- Lee, ThaeMin, (2005), the impact of perceptions of interactivity on customer trust and transaction intentions in mobile commerce, Journal of Electronic Commerce Research, VOL. 6, NO.3, (pp.165-180), Busan, Korea.
- 15- Maiwald, Eric, (2003), Network Security A Beginner's Guide, 2nd Edition, The McGraw-Hill Companies, USA.
- 16- McClure, Stuart & Scambray, Joel & Kurtz, George, (2007), Hacking Exposed™ 6: Network Security/Secrets & Solutions, 10th Anniversary Edition, The McGraw-Hill Companies, USA.
- 17- Nakrem, Are, (2007), Managing Information Security in Organizations-A Case Study, Master Thesis , Faculty of Economics and Social Sciences, Agder University College.
- 18- Nampanda, Kondwani (2000), Identifying Best Practices for Security in Patient Health Information Systems (E-health Solutions) in Resource Limited Setting-Malawi Case on Establishment of National Health Data Repository Centre,

Master Thesis, Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology.

19- Osborne, (2006), Mark How to Cheat at Managing Information Security, Syngress Publishing, Inc.

20- Pathan, Al-Sakib Khan,(2011), Security of Self Organizing Networks, 2011 by Taylor And Francis Group, LLC, USA .

21- Pettersson, Göran, (2008), Defining Information Security As a Policy, Bachelor Thesis, Software Engineering and Management, IT University of Göteborg.

22- Puangsri, Panchit ,(2001), Quantitative Return On Information Security Investment/ A Model For Cost Benefit Analysis, Master Thesis, Department Of Technology, Policy And Management, Delft University Of Technology.

23- Putri, Nia Ramadiani & Mganga, Medard Charles, (2011), Enhancing Information Security in Cloud Computing Services using SLA Based Metrics master thesis , school of computing, Belkinge Institute of technology, Sweden.

24- Sarwar, Muhammad Zaman & Abbasi, Kashif Shafique & Pervaiz, Saleem, (2012), The Effect Of Customer Trust On Customer Loyalty And Customer Retention: A Moderating Role Of Cause Related Marketing, Global Journal Of Management And Business Research, Volume 12, Issue 6 , Version 1.0, Global Journals Inc. (USA).

25- Sirdeshmukh, Deepak and Singh, Jagdip and Sabol ,Barry, 2002, Consumer Trust, Value, and Loyalty in Relational Exchanges, Journal of Marketing, Vol. 66, No. 1 ,American Marketing Association, (pp. 15-37).

26- Soderbom, Jonas, (2007), The Costs Of Enterprise Information Security/A Relative Assessment Approach , Master Thesis, Industrial Information And Control Systems Department, KTH Royal Institute Of Technology, Stockholm, Sweden.

27- Suh , Bomil and Han, Ingoo,(2003), The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce, International Journal of Electronic Commerce, Vol. 7, No. 3, Taylor & Francis, Ltd, (pp. 135-161).

28- Upamannyu, Nischay K. & Gulati , Chanda & Chack, Ankita & Kaur, Gurvinder, (2015), The Effect Of Customer Trust On Customer Loyalty And Repurchase Intention: The Moderating Influence Of Perceived Csr , International Journal Of Research In It, Management And Engineering, Volume 5, Issue 4, (Pp.1-31).

29- Van Niekerk, (2010) Johannes Frederick, fostering information security culture through integrating theory and technology, PHD thesis in information technology, Faculty of Engineering, the Built Environment and Information Technology, Nelson Mandela Metropolitan University.

30- van Opstal, ir. A.A.M.,(2008),A Structured Approach to Software Security, master thesis, TiasNimbis Business School.

31- Vuuren, T. van M. and Lombard Roberts- & Tonder ,E. van, 2012, Customer satisfaction, trust and commitment as predictors of customer loyalty within an optometric practice environment, Southern African Business Review Volume 16 Number, (pp. 81-96).

32- Wallin, Emil & Xu, Ying, (2008), Managing Information Security in Healthcare: A Case Study in Region Skåne, master thesis, Department of Informatics, school of informatics and economics, Lund university.

33- Zegers, Nanno , (2006), A Methodology For Improving Information Security Incident Identification And Response, Master Thesis Informatics & Economics, Master Thesis Informatics & Economics, Faculty Of Economics, Erasmus University Rotterdam.