مجلة تنمية الرافدين

اسم المقال: فاعلية التدريب في تحقيق نجاح أمن نظم المعلومات دراسة استطلاعية لآراء عينة من العاملين في نظم المعلومات بجامعة الموصل
اسم الكاتب: أ.م. رائد عبدالقادر حامد الدباغ، بشرى علي زينل
رابط ثابت: https://political-encyclopedia.org/index.php/library/3466
تاريخ الاسترداد: 2026/11/02 21:39 +03

الموسوعة السياسيّة هي مبادرة أكاديمية غير هادفة للربح، تساعد الباحثين والطلاب على الوصول واستخدام وبناء مجموعات أوسع من المحتوى العلمي العربي في مجال علم السياسة واستخدامها في الأرشيف الرقمي الموثوق به لإغناء المحتوى العربي على الإنترنت.
لمزيد من المعلومات حول الموسوعة السياسيّة - Encyclopedia Political، يرجى التواصل على info@political-encyclopedia.org

استخدامكم لأرشيف مكتبة الموسوعة السياسيّة - Encyclopedia Political يعني موافقتك على شروط وأحكام الاستخدام المتاحة على الموقع https://political-encyclopedia.org/terms-of-use

تم الحصول على هذا المقال من موقع مجلة تنمية الرافدين كلية الإدارة والاقتصاد / جامعة الموصل ورفده في مكتبة الموسوعة السياسيّة مستوفياً شروط حقوق الملكية الفكريّة ومتطلبات رخصة المشاع الإبداعي التي ينضوي المقال تحتها.

كلية الإدارة والاقتصاد -جامعة الموصل تنمية الرافدين ملحق العدد ١١٠ مجلد ٣٤ لسنة ٢٠١٢
ص ص[١٢٣ -١٤٠]

فاعلية التدريب في تحقيق نجاح أمن نظم المعلومات
دراسة استطلاعية لآراء عينة من العاملين في نظم المعلومات بجامعة الموصل*

رائد عبدالقادر حامد الدباغ
استاذ مساعد - قسم نظم المعلومات الإدارية
raiddabagh@yahoo.com

بشرى علي زينل
ماجستير
Bushbush2011287@yahoo.com

كلية الإدارة والاقتصاد - جامعة الموصل

المستخلص

تسعى هذه الدراسة إلى بيان مدى فاعلية التدريب ومساهمته في تحقيق النجاح للعاملين في نظم المعلومات وحمايتها، وتهدف إلى تحديد مدى توافر المعلومات والخبرة الشخصية لدى الأفراد، مع تحديد مدى توافر البنى التحتية والإمكانات المادية والبرمجية، ومدى توافر التشريعات القانونية التي تدعمها. واعتمدت الدراسة في جانبها العملي المنهج الوصفي التحليلي، إذ تم توزيع ٥٥ استمارة استبانة على مجموعة من العاملين في مجال نظم المعلومات من منتسبي جامعة الموصل. وكان من أهم نتائجها: وجود تباين على مستوى الجنس والخبرة العملية المباشرة في إجابات أفراد العينة حول موضوع أمن المعلومات، في حين لم تظهر النتائج أي تباين في إجابات العينة من المتدربين وغير المتدربين حول هذا الموضوع. وخرجت الدراسة بمجموعة من التوصيات التي يمكن الإفادة منها لتطوير البرامج التدريبية في مجال أمن المعلومات.

الكلمات المفتاحية:
نظم المعلومات، أمن نظم المعلومات، فاعلية التدريب.

* بحث مستل من رسالة الماجستير الموسومة "***تصميم معلومات مستند على الويب باعتماد الشبكة الافتراضية الخاصة- دراسة حالة في مصرف الرشيد***"، مقدمة الى مجلس كلية الادارة والاقتصاد، جامعة الموصل، غير منشورة.

تأريخ استلام البحث ٢٠١٢/٦/١٤ تأريخ قبول النشر ٢٠١٢/٩/٢٤

Training Effectiveness in Achieving the Success of Information Systems Security
Exploratory Study of the Views of a Sample of Workers in Information Systems at University of Mosul

Raid A. Al-Dabbag
Assistant Professor
Department of Management Information System
University of Mosul
raiddabagh@yahoo.com

Bushra A. Zaynal
Researcher
Department of Management Information System
University of Mosul
Bushbush2011287@yahoo.com

Abstract

This study aims to demonstrate the extent of effectiveness of the information systems training, and its contribution in the success of information systems security and protection. The study aims to identify the availability of information and personal experience of trained and untrained individuals, and to identify the availability of infrastructure and potentials of hardware and software in the organization, and the availability of legal legislation that supports it. This study depended in its practical side a descriptive analytical method. Fifty five questionnaires were distributed on a group of workers in the area of information systems, the most important result is the existence of variation in the level of gender and direct practical experience in the answers on the topic of information security, while the results did not show any variation in the answers of the trained and untrained individuals, finally this study came out with a set of recommendations that can be utilized in developing information security training programs.

Keywords :
Information Systems, Information Systems Security, Training Effectiveness.

المقدمة

تعد نظم المعلومات الإدارية من أبرز أنواع نظم المعلومات لتأثيرها الكبير في تنظيم المعلومات المنظمية بشكل يضمن الحصول على المعلومات الضرورية للمنظمة والتي تمكنها من السيطرة في مجال عملها والتفوق على المنافسين، ولأهمية هذه الأنظمة لابد من توفير آلية يتم بها حماية أنظمة المعلومات، وأبرز وسيلة لذلك تتمثل بأمن نظم المعلومات، وذلك من خلال تشخيص نقاط الضعف في أنظمة المعلومات والتي تمكن المخترقين من الإستفادة منها للقيام بتغييرات في هذه النظم. ويعد التدريب من ابرز الاساليب التي يمكن من خلالها حماية وتأمين نظم المعلومات، إذ تعد الكوادر المدربة على استخدام ادوات وتقانات الحماية الفعالة لنظم المعلومات من أبرز هذه الأساليب، لذلك لابد من توفير مناهج تدريبية تساعد على تقوية المعلومات والخبرات التي يحصل عليها الفرد في مجال عمله، أو من خلال قراءاته وصقلها وتوجيهها بالإتجاه الصحيح نحو توفير نظم معلومات محمية من أي نوع من أنواع الإختراقات أو التغييرات.

مشكلة الدراسة

تتناول الدراسة الحالية مدى فاعلية التدريب في مجال تقانة المعلومات وأثره في تحقيق نجاح أمن نظم المعلومات، ويمكن توضيح مشكلة الدراسة من خلال التساؤلات البحثية الآتية:

١. ما مدى اطلاع العاملين في نظم المعلومات المختلفة على مفهوم أمن نظم المعلومات؟
٢. هل تتوافر لدى الأفراد المبحوثين المعلومات والخبرات الكافية والتي تفيدهم في مجال حماية أنظمة المعلومات؟
٣. هل تتوافر مناهج فعالة للتدريب تركز على أمن نظم المعلومات؟
٤. في حالة توافر المعلومات الكافية لدى الأفراد المبحوثين في مجال أمن نظم المعلومات، هل تتوافر لدى المنظمة المبحوثة الإمكانات والبنى التحتية والتشريعات القانونية التي تدعم تطبيق هذه المعلومات على أرض الواقع؟

أهمية الدراسة

تكمن أهمية الدراسة في تناولها لأحد الموضوعات الحيوية في الوقت الحالي، الا وهو أمن نظم المعلومات، والذي أغفلته معظم المنظمات على الرغم من أهميته الكبيرة، ومسأهمته في تحقيق النجاح للمنظمة، وحماية المعلومات التي تعد المورد الأساسي الذي تعتمد عليه المنظمة.

وبالتركيز على مدى فاعلية التدريب في هذا المجال من الممكن التمييز مابين الأفراد العاملين في أنظمة المعلومات سواء أكانوا متدربين أم غير متدربين، ويمكن تحديد أهمية الدراسة من خلال الآتي:

١. بيان مدى فاعلية المناهج التدريبية التي توفرها الأكاديميات الخاصة بالتدريب في مجال تقانة المعلومات ومساهمتها في تحقيق نجاح أمن نظم المعلومات.
٢. يتوقع أن تسهم الدراسة في زيادة الانتباه إلى أهمية دعم البرامج التدريبية والتأهيلية، بمناهج تركز على أمن نظم المعلومات في المنظمات.
٣. تسهم في توفير دراسة استطلاعية تدعم الجانب النظري من أجل حماية توفير أمن وحماية أفضل لنظم المعلومات.

أهداف الدراسة

تسعى هذه الدراسة لتحقيق الأهداف الآتية:

١. التعرف على مفهوم أمن نظم المعلومات، فضلاً عن تحديد مواضع الضعف في نظم المعلومات والتي يمكن استغلالها من قبل المخترقين، بالإضافة إلى تحديد الأدوات والتقانات الضرورية لتزويد النظم بآليات الحماية الفعالة ضد أي أخطار أو تهديدات محتملة.
٢. تحديد مدى فاعلية التدريب في مجال تقانة المعلومات، ومدى تركيزه على موضوع أمن نظم المعلومات.
٣. تحديد مدى توافر المعلومات والخبرات الشخصية في مجال أمن نظم المعلومات.
٤. تقديم توصيات مستقبلية يمكن الإفادة منها من قبل أنظمة المعلومات، فضلاً عن المسؤولين عن الدورات التدريبية لكوادر نظم المعلومات.

فرضيات الدراسة

سنعرض فرضيات الدراسة من خلال تقسيمها على قسمين، الأول يمثل الجزء الخاص بالفرد وخبرته في مجال نظم المعلومات، والثاني الجزء الخاص بالمنظمة التي يعمل فيها ومدى توافر الإمكانات المادية والتشريعية، بالإضافة إلى البنية التحتية، وسيتم عرض هذه الفرضيات بحسب كل جزء وعلى النحو الآتي:

الفرضية الأولى: لايوجد تباين في إجابات أفراد عينة البحث فيما يخص المعلومات الشخصية والخبرة في مجال أمن نظم المعلومات.

الفرضية الثانية: لايوجد تباين في إجابات أفراد عينة البحث بخصوص مدى توافر الإمكانات المادية والبرمجية والتشريعات القانونية التي تدعم عمل المنظمة.

أولاً- أمن نظم المعلومات

تتضمن خدمات أمن المعلومات الكثير من التعقيد بسبب تنوع الشبكات الكبيرة والمفتوحة وتعرضها إلى هجمات وتهديدات كبيرة نتيجة لتطور التقانات المستخدمة في هذه الشبكات بشكل مستمر (Sen, 2012, 337).

إن كوادر أمن نظم المعلومات عادة ما يكونوا من ذوي الخلفية الذهنية الواسعة، ولكن معظمهم لايملك وعياً أو تدريباً في مجال التحليل المنظمي أو المجتمعي، وبالتالي فإنهم قد يقللوا من أهمية أو يبالغوا في تقدير الخطر (Kreicberga, 2010, 2).

كما إن أمن نظم المعلومات يحتاج إلى تعاون كامل من كوادر الموظفين كافة، وذلك لغرض تطبيق سياسات أمن نظم المعلومات التي تضعها الإدارة (Puhakainen, 2006, 34).

وبما أن متطلبات أمن نظم المعلومات قد تنتج من بيئة المنظمة، من هنا لابد من تعريف وتطبيق الضوابط الأمنية الصارمة للتأكد من حماية موارد المعلومات من التهديدات المحتملة (Hutchison *et al.*, 2005, 157).

وأحد أهم مجالات أمن نظم المعلومات يتعلق بالحماية من فقدان البيانات والتأكد من وجودها، إذ أن البيانات عادة ما تكون مكتوبة على وسائط التخزين، وهذه الأقراص قد يصيبها خلل يؤدي إلى فقدان هذه البيانات، أو وجودها (Millar and Gregg, 2007, 145).

١- مفهوم أمن نظم المعلومات

ويمكن توضيح مفهوم أمن نظم المعلومات من خلال الجدول الآتي:

الجدول ١

مفهوم أمن نظم المعلومات من وجهة نظر الكتاب والباحثين

الباحث/ الكاتب، السنة، الصفحة	المفهوم
(ياسين، ٢٠٠٨ ، ٢٥١)	يعني كل السياسات والإجراءات التي تستخدم لحماية النظام من كل أشكال التخريب، الإضرار، وانتهاك حرمة البيانات والمعلومات فضلاً عن حماية النظام من التهديدات الطبيعية أو العادية.
(Nachatigal,2009 , 136)	وهي مجموعة من الإجراءات والمقاييس الممكنة لنظم المعلومات التي تعطيها القدرة على مواجهة المتطلبات الأمنية المعرفة بشكل مسبق.

الباحث/ الكاتب، السنة، الصفحة	المفهوم
(Oscarson, 2007 , 98)	إن أمن نظم المعلومات يمكن التعبير عنه بالحالة التي تكون فيها أصول المعلومات موثوقة وصحيحة ومتوافرة.
(Stojakovic, 2000 , 31)	تشير حماية أو أمن نظم المعلومات اليوم إلى مجالين رئيسين، الوقاية والحماية الفعالة، حيث إن الوقاية تتضمن كل المقاييس المستخدمة عند حدوث أي طارئ أمني، أما الحماية الفعالة فتتضمن الطرائق والأدوات التي توفر الأمن والحماية في الوقت الحقيقي.
(Nakrem, 2007 , 3)	عرف من قبل قاموس مصطلحات أمن نظم المعلومات على أنه حماية نظم المعلومات من الوصول غير المخول للمعلومات، أو التعديل على المعلومات سواءاً أكانت مخزنة أم تتم معالجتها أو يتم نقلها، والحماية أيضاً من الحرمان من الخدمة للمستخدمين المخولين.
(Jessup&Valacich,2008,232)	يشير إلى أخذ التدابير الوقائية، للإبقاء على كافة مجالات نظم المعلومات، (مثل: المكونات المادية والبرامجيات والمعدات الشبكية والبيانات) محمية من الدخول أو الاستخدام غير المخول.
(Dhillon, 1995 , 17)	لايهتم أمن نظم المعلومات بالأمن التقاني ككل، وإنما يهتم أيضا بأمن النظم الرسمية وغير الرسمية ضمن المنظمة، إذ أن النظم الرسمية تحكم بقواعد معينة، والفرق مابين النظم الرسمية وغير الرسمية يمكن تحديده من قبل متخذ القرار.

المصدر: من اعداد الباحثين بالاعتماد على المصادر الواردة فيه.

٢- أساسيات أمن نظم المعلومات

هنالك مجموعة من المفاهيم الأساسية التي يترافق استخدامها مع أمن نظم المعلومات وتتضمن التهديدات والخطر، والثقة ذات العلاقة بأمن نظم المعلومات ويمكن توضيح هذه المواضيع بالآتي:

أ. التهديدات لأمن نظم المعلومات: إن أصول المعلومات تتألف من المعلومات وأية موارد تستخدم لإدارة هذه المعلومات، وهذه الأصول عادة ما تكون معرضة للتهديدات ويمكن توضيح مفهوم التهديدات في مجال الحواسيب، وتقانة المعلومات وأمن نظم المعلومات على أنها "أية أخطار محتملة على المعلومات أو الأنظمة" (Oscarson, 2007 , 101).

ويمكن تصنيف التهديدات بحسب مختبر الأبحاث Naval على أساس مصدرها إلى (التهديدات المتعمدة والتهديدات غير المتعمدة)، ووقت ظهور التهديد (أثناء التطوير، أو الصيانة، أو التشغيل)، أو موقع التهديد سواء أكان يستهدف البرامجيات أو المكونات المادية (Farahmand, 2004 , 53).

وتمثل التهديدات مدى واسعاً من القوى القادرة على التسبب بعواقب سلبية، إذ يتسبب التهديد بانتاج الخطر من خلال القدرة أو القابلية على جعل قوة معينة في سياق نظم المعلومات تعمل بشكل مضر لهذه النظم، إذ أن التهديدات يمكن أن تكون داخلية أو خارجية، بشرية أو غير بشرية، عرضية أو غير عرضية (Schuessler, 2009, 12).

وتستخدم التهديدات مجموعة من الأدوات والبرامج للقيام بالهجمات على الشبكات مثل الهجمات على الخوادم وأجهزة الحواسيب، والتهديدات على أمن الشبكات في نظم المعلومات يمكن ان تصنف على تهديدات داخلية أو خارجية، مهيكلة أو غير مهيكلة (Baral, 2010 , 9).

ب. الخطر في أمن نظم المعلومات: إن التحليل الإحصائي لأمن وجرائم الحاسوب عادة مايتم عرقلته بسبب قلة استجابة ضحاياه، والسبب يعود إلى أن معظم المنظمات ترفض الاعتراف بالمشاكل الأمنية لإدراكها بأن عامة الناس ستفقد ثقتها بالمنظمة، حال إكتشافها لوجود مثل هذه المشاكل (Burnburg, 2003, 17).

يعرف الخطر في مجال استغلال نقاط الضعف لنظم المعلومات على أنه "فقدان القدرة أو القابلية نتيجة لوجود تهديد معين يستغل نقطة ضعف معينة لنظم المعلومات، والخطر في مجال أمن نظم المعلومات يكون متوقع ويمكن قياسه (Oscarson, 2007, 112).

وهنالك بعض المخاطر يقوم من خلالها المهاجمين بالدخول إلى محتويات البريد الإلكتروني، وبعض محتويات البريد الإلكتروني قد تكون حساسة بطبيعتها (Hutchison, 2011, 311).

والخطر أيضاً يمكن أن يكون مشتركاً مابين المنظمات، فعندما يتم الاعتماد على المصادر الخارجية للحصول على خدمات تقانة المعلومات، فإن الأمن يمكن أن يكون أحد القضايا الاساسية لكل من المنظمات وزبائنها، إذ أن النظام يكون أمناً بقدر أمن بائعيه ومزودي خدماته (Braynt, 2007, 40).

ت. الثقة ذات العلاقة بأمن نظم المعلومات: تعد الثقة من أبرز المجالات البحثية في علوم الحاسوب، وإن الثقة توضح من خلال طرفين يرتبطان مع بعضهما من خلال عمل معين، حيث يفهمان بعضهما البعض بطريقة معينة تسمح للعلاقة بينهما أن تصل إلى النتائج المرجوة (Zissis, 2011, 99).

ومن جانب آخر فإن المستخدمين للشبكات الاجتماعية يميلون عادة إلى الوثوق ببعضهم البعض أكثر من المستخدمين العشوائيين في الشبكات الاخرى (Mislove, 2009, 19).

وتعد الثقة من العوامل التي تقلل المخاطر المفترضة من قبل أحد اطراف عملية تجارية معينة مع الطرف الاخر للعملية نفسها، وكلما زادت الثقة فان الخطر اما أن يقل أو يصبح بالامكان السيطرة عليه من قبل اطراف العملية (Bener, 2000, 45).

والثقة من المتطلبات الضرورية للتفاعل مابين الأطراف التي تجهل بعضها البعض، إذ يعد التحقق من موثوقية العمليات الإلكترونية أحد أهم جوانب التعاون الموثوق ما بين نظم المعلومات المستندة إلى الانترنت (Jacobsson, 2008, 152).

تشير الثقة إلى التكاملية والإبقاء على المعلومات المتمتعة بالموثوقية بشكل سري، وأداء وإنجاز الوظائف المطلوبة بشكل مستمر، إن الثقة لا تعتمد فقط على النظام وإنما على الأفراد المستخدمين له، وهذا يدل على أن الثقة تعد من المفاهيم صعبة القياس (Stjerneby, 2002, 27).

إن طبيعة أمن نظم المعلومات تفرض علينا وجود نوعين أساسيين من الثقة، الثقة الإجتماعية، والثقة التقانية والتي يمكن توضيحها بالآتي (Oscarson, 2007, 118):

- الثقة الإجتماعية: إن الثقة في العلاقات الإنسانية عادة مايطلق عليها بالثقة التفاعلية، وفي العلاقات مابين منظمات الأعمال يمكن الحديث عن ثقة شركاء الأعمال، كجزء من العلاقات التفاعلية المنظمية.
- الثقة التقانية: إن كل طرف من اطراف العلاقة المنظمية يجب أن يثق بالبنية التحتية التقانية الداخلية للطرف الآخر، ويمكن استخدام العديد من الآليات الأمنية مثل التشفير وجدران النار للوصول إلى المستويات الأمنية المطلوبة وزيادة الثقة بالبنية التحتية ونظم المعلومات.

٣- قابلية إختراق نظم المعلومات

عند تخزين كميات كبيرة من البيانات بشكل الكتروني، فإنها تصبح عرضة للعديد من أنواع التهديدات مقارنة بتلك المخزونة بشكل يدوي، وعلى الرغم من أن شبكات الإتصالات ونظم المعلومات تكون مترابطة، فإن احتمالية الدخول غير المخول، لا تكون محصورة بموقع معين بل إنها يمكن أن تصيب كل نقطة وصول في الشبكة (Laundon and Laundon, 2009 , 231).

ويمكن التمييز مابين قابلية الإختراق والتهديدات من حيث أن قابلية الإختراق هو مواطن الضعف المتواجدة في أمن النظم وإجراءاتها وتصميمها وتطبيقها وضوابطها والتي يتم استغلالها لانتهاك السياسة الأمنية للنظم، إذ أن التهديدات تعد عامة أما قابلية الإختراق فتعد خاصة ببيئات معينة بما أنها تعتمد على المعايير الأمنية المستخدمة في النظام (Nachtigal, 2009 , 83).

ويمكن أن تمثل التهديدات مدى واسع من القوى التي تنتج عنها عواقب وخيمة، إذ يصبح التهديد خطراً من خلال القدرة أو القابلية على جعل قوى معينة قادرة على العمل بصورة تحدث ضرراً بنظم المعلومات (Schuessler, 2009 , 12).

إن نظم المعلومات تتعرض إلى العديد من المخاطر والتي يمكن إيضاحها من خلال الآتي (Jessup and Valacich, 2008 , 233):

١. **الدخول غير المخول:** إن هجمات الدخول غير المخول تحدث عند دخول المستخدمين غير المخولين، والتلاعب بالمعلومات، أو التجسس على أجهزة المرقاب (Monitors) التي تتضمن معلوماتها الموثوقة.
٢. **التعديل على المعلومات:** يحدث التعديل على المعلومات عند دخول أحد الأفراد على المعلومات الإلكترونية، وتغيير هذه المعلومات بطريقة معينة.
٣. **الحرمان من الخدمة:** يحدث عند تعمد المتسللين الإلكترونيين على منع المستخدمين المخولين لخدمة معينة من استخدام هذه الخدمة.
٤. **فيروسات الحاسوب:** إذ تدمر الفيروسات البيانات، وتستهلك وقت الأفراد وأموالهم ومواردهم نتيجة لمحاولتهم إصلاح الأضرار التي تسببها.
٥. **برامج التجسس أو الإغراق:** حيث إن برامج التجسس Spyware هي برامج تجمع معلومات عن مستخدم معين مرتبط بالانترنت من دون علم المستخدم، أما برامج الإغراق Spam فهي تغزو البريد الإلكتروني، وهي رسائل بريد الكتروني غير مرغوبة، حيث تستهلك احجاماً كبيرة من مساحة التخرين وتستنفذ عرض الحزمة المخصصة للشبكة.

ومن جانب آخر، فإن قابلية الإختراق لنظم المعلومات هي نقاط الضعف في نظم المعلومات، إذ أن قابلية الإختراق عادة ماتكون جزءاً من أحداث سلبية، وذلك لأن نقاط الضعف المتواجدة في النظم والتي تفسح المجال للأختراق عادة ما تكون عواقبها سلبية (Bryant, 2007 , 23).

فضلاً عن ماسبق، فإن زيادة تعقيد وتنوع المكونات المادية، والبرامجيات، ذات العلاقة بالأفراد والمنظمات التي تحتاجها شبكات الإتصالات أدى إلى نشوء مجالات وفرص جديدة للإختراق والتلاعب، إذ أن الأجهزة اللاسلكية يمكن أن تنشأ شبكات متخصصة تستغل من قبل الكيانات الخبيثة، بالإضافة إلى تعطيل الخدمات (Laundon and Laundon, 2002 , 434).

وتعد الشراكات المحلية أو الخارجية مع الجهات الأخرى من أبرز مواطن الضعف وقابلية الإختراق، وخصوصاً في حالة وجود معلومات قيمة في الشبكات والحواسيب الخارجة عن سيطرة المنظمة، ومن دون الوقاية فان البيانات القيمة يمكن أن تفقد أو تدمر (Laundon and Laundon, 2010 , 324).

ويمكن توضيح قابليات الإختراق للمعلومات الحساسة من خلال الجدول الآتي:

الجدول ٢
قابليات اختراق المعلومات الحساسة

الخصائص	الهدف	نوع الإختراق
التحقق من الهوية	واجهة المستخدم	انتحال الشخصية التوقع الاحتيال
الموثوقية	مخازن معلومات قنوات الإتصالات	التجسس الإعتراض أو التأخير
الملكية	مخازن المعلومات	سرقة جلسات الحوار
التكاملية	مخازن معلومات قنوات الإتصال	التزييف التزوير
المنفعة	مخازن المعلومات	الإضرار بالممتلكات (أي فقدان مفاتيح التشفير بالصدفة للنسخة المشفرة الوحيدة للمعلومات المهمة

Source: Wu, 2009, Security Architecture for Sensitive Information Systems, PHD Thesis, Faculty Of Information Technology, Monash University, Australia, P.7

ثانياً - التدريب

يعد التدريب أحد القدرات البشرية الفطرية التي يمكن تطويرها حتى تصل إلى مستوى عالي من الحرفية، والتدريب في الأصل هو شكل من اشكال التنمية البشرية التي يساعد فيها المدرب على اكتشاف قدرات الفرد، ويمارس المدرب هذا الدور بأستخدام أساليب ومناهج تهدف إلى دعم الفرد وتشجيعه، وفوق هذا تشعره بضرورة تحمله مسؤولية تنمية نفسه بشكل مباشر (العامري، ٢٠٠٧، ١٩).

ولقد ظهرت العديد من التعاريف للتدريب ومن أبرزها عملية تزويد الأفراد أو الجماعات بالمعلومات والخبرات والمهارات وطرق الاداء والسلوك بحيث يكون هؤلاء الأفراد أو الجماعات قادرين على القيام بوظائفهم بفاعلية وكفاءة (السكارنة، ٢٠٠٩، ١٨).

ومن ابرز متطلبات التدريب الفعال الاخذ بنظر الاعتبار مجموعة من الاعتبارات منها الاتي (مالكوم بيل، ١٩٩٧، ٤٥):

١. **الإعتبار المالي:** قد تختلف التكاليف وفقاً لاختلاف الأساليب التدريبية المتُبعة لتحقيق الاهداف ذاتها، وهنا يعتمد الخيار على الظروف الفردية، ولا توجد طريقة مختصرة إلى التقييم الملائم للأساليب المعروضة، وتشمل التكاليف الكاملة للتدريب، تكاليف الاشتراك في التدريب، وتكاليف واجور ورواتب المدربين، وتكاليف خاصة بالاشراف على التدريب.
٢. **الإعتبار الزمني للتدريب:** قد يكون عامل الزمن مهما بطرق مختلفة، فتدريب الموظفين لوظيفة جديدة يخضع لضغوط الوقت، ومن مصلحة الجميع أن يكون التدريب بأسرع

ما يمكن وقد توجد مواعيد نهائية للتدريب وتشمل هذه المواعيد ضرورة تجهيز آلات ومعدات جديدة أو إطلاق سلعة جديدة.

٣. **إختيار المدرب:** هنالك العديد من الخيارات لاختيار المدربين منها، اختيار مدربين من داخل المنظمة، أو مستشارين تدريبيين من خارج المنظمة، أو من الكليات أو الجامعات المحلية، والهيئات المتخصصة بالتدريب، والمدراء في العمل المطلوب، والزملاء في العمل.

٤. **مكان التدريب وتجهيزاته:** من المفترض ان تكون كل الاساليب التدريبية مزودة بأمكنة وتجهيزات خاصة بالتدريب ومكاناً تدريبياً ملائماً فضلاً عن الأثاث الملائم والتجهيزات الأساسية، حيث إن معظم اساليب التدريب التي تحصل خارج مكان العمل تتطلب حداً ادنى من التجهيزات مثل الشاشات وغيرها.

أما التدريب الخاص بتقانة المعلومات فيمكن تعريفه على أنه دراسة وتصميم وتطوير وتطبيق ودعم وإدارة لنظم المعلومات المستندة الى الحاسوب، وبالأخص التطبيقات الخاصة بالبرامجيات، والمكونات المادية للحاسوب، وهذا ما يقود إلى مدى واسع من الفرص الخاصة بالتدريب، وبالنسبة للتدريب المتخصص في مجال الأمن،فقد قسّم المعهد القومي الأمريكي للمعايير والتكنولوجيا البرامج التدريبية الضرورية في هذا المجال إلى التدريب على المعرفة أو الوعي، والتدريب المهاري، والتدريب على التعليم، حيث إن المعرفة أو الوعي الأمني يعد الأساس لأي تدريب في مجال الأمن، وتستخدم لتزويد الفرد بالمعلومات الكافية لغرض تمييز المشاكل الأمنية المحتملة، هذا بالنسبة للمستوى الأول اما المستوى الثاني والمتمثل بالتدريب المهاري فانه يركز على تعليم المهارات الضرورية للأفراد لإنجاز وظائفهم بطريقة آمنة، أما المستوى الثالث في التدريب الأمني فيتعلق بالتعليم، والذي يكون أعمق من التدريب الأمني، ويستهدف الخبراء الأمنيين والأفراد الذين تتطلب أعمالهم خبرة في مجال الأمن (Phelps, 2005 ,59).

ثالثاً- نتائج الدراسة

١- وصف متغيرات الدراسة وتشخيصها

تم توزيع ٥٥ استمارة استبانة على مجموعة من العاملين في مجال نظم المعلومات، وكانت هذه العينة تتضمن ٣٣ فرداً من المتدربين في أكاديمية سيسكو/جامعة الموصل و٢٢ فرداً من غير المتدربين في الأكاديمية وبعد إجراء التحليل الإحصائي لهذه الاستمارات تم استخراج النتائج المتعلقة بالأسئلة الخاصة بالمعلومات الشخصية للفرد وخبرته في مجال نظم المعلومات والتي يمكن إيضاحها من خلال الجدأول ٣-٨ والتي تمثل مستويات مختلفة تشمل التدريب والجنس والخبرة العملية وعدد سنوات الخدمة التي قضاها في عمله الحالي، وعدد ساعات العمل الأسبوعية وعلى النحو الآتي:

الجدول ٣
وصف لافراد عينة الدراسة من حيث الجنس

الجنس	ذكر		أنثى	
	ت	%	ت	%
	٣٣	٦٠.٠٠	٢٢	٤٠.٠٠

المصدر : من اعداد الباحثان بالاعتماد على نتائج الحاسوب.

ونلاحظ من خلال الجدول أعلاه أن نسبة الإناث من عينة الدراسة بلغت ٤٠% ونسبة الذكور بلغت ٦٠%.

الجدول ٤
وصف لافراد عينة الدراسة من حيث الفئة العمرية

الفئة العمرية	مافوق ١٨		١٨-٢٤		٢٥-٣٤		٣٥-٤٤		٤٥-٥٤		٥٥-٦٤		ما فوق ٦٥ سنة	
	ت	%	ت	%	ت	%	ت	%	ت	%	ت	%	ت	%
	-	--	٢	٣.٦٤	٢٣	٥٨.١٨	٣٢	٥٨.١٨	١٦	٢٩.٠٩	٣	٥.٤٥	٢	٣.٦٤

المصدر : من اعداد الباحثان بالاعتماد على نتائج الحاسوب.

أما الفئة العمرية للأفراد المبحوثين فقد كانت النسبة الأكبر منهم من ٢٥-٣٤ سنة، وأقل نسبة من الفئات العمرية كانت في فئة من ١٨-٢٤.

الجدول ٥
وصف لأفراد عينة الدراسة من حيث التدريب والتأهيل

التدريب والتأهيل	المتدربين		غير المتدربين	
	ت	%	ت	%
	٤١	٤٧.٥٥	١٤	٢٥.٤٥

المصدر : من اعداد الباحثان بالاعتماد على نتائج الحاسوب.

ويلاحظ من خلال الجدول ٥ انه قد بلغت نسبة المتدربين في أكاديمية سيسكو ٤٧.٥٥%، وغير المتدربين ٢٥.٤٥%.

الجدول ٦
وصف لافراد عينة الدراسة من حيث السنوات التي قضاها في عمله الحالي

عدد السنوات عمل الفرد الحالي	١سنة		١-٢ سنة		٣-٥ سنة		٦-١١ سنة		١١-١٥ سنة		١٦-٢٠ سنة		٢٠ فمافوق	
	ت	%	ت	%	ت	%	ت	%	ت	%	ت	%	ت	%
	٣	٥.٤٥	٧	١٢.٧٣	١٧	٣٠.٩١	٢٢	٤٠.٠٠	--	---	٣	٥.٤٥	٣	٥.٤٥

المصدر : من اعداد الباحثان بالاعتماد على نتائج الحاسوب.

وبلغت أعلى نسبة في عدد سنوات الخدمة لعينة الدراسة في الفئة من ٦-١١، إذ بلغت ٤٠%، أما أدنى نسبة فكانت في فئة سنة واحدة وبلغت نسبتها المئوية من عينة الدراسة ٥.٤٥%.

الجدول ٧
الخبرة العملية المباشرة في مجال نظم المعلومات

الخبرة العملية المباشرة في نظم المعلومات	واسعة		متوسطة		واسعة	
	ت	%	ت	%	ت	%
	١٦	٢٩.٠٩	٣٧	٦٧.٢٧	٢	٣.٦٤

المصدر : من اعداد الباحثان بالاعتماد على نتائج الحاسوب.

بلغت أعلى نسبة من الإجابات حول هذه الفقرة ٦٧.٢٧% والتي تمثل الإجابة بأن الخبرة العلمية المباشرة في نظم المعلومات كانت متوسطة، في حين إن النسبة المئوية لعدد الأفراد الذين يملكون خبرة واسعة في مجال الخبرة العلمية المباشرة كانت متدنية، إذ بلغت ٣.٦٤% .

الجدول ٨
وصف لأفراد العينة من حيث عدد الساعات الأسبوعية التي يقضيها في العمل المرتبط بنظم المعلومات

عدد الساعات الاسبوعية التي يقضيها الفرد في نظم المعلومات	١ ساعة		١-٢ ساعة		٣-٥ ساعة		٦-١٠ ساعة		١٦-٢٠ ساعة		أكثرمن ٢٠ ساعة	
	ت	%	ت	%	ت	%	ت	%	ت	%	ت	%
	١	١.٨٢	٤	٧.٢٧	١٥	٢٧.٢٧	٢٠	٣٦.٣٦	٥	٩.٠٩	١٠	١٨.١٨

المصدر : من اعداد الباحثان بالاعتماد على نتائج الحاسوب.

في حين كانت الفئة الأكبر من عينة الدراسة تقضي ما نسبته ٣٦.٣٦% أي ٦-١٠ ساعات أسبوعياً في العمل المرتبط بنظم المعلومات، في حين كانت النسبة الأقل (١.٢٨%) من عينة الدراسة تقضي وقتاً ما بين ١٦- ٢٠ ساعة أسبوعياً.

١. إيجاد النسب المئوية والوسط الحسابي لإجابات عينة الدراسة: وقد تضمن الجزء الثاني من استمارة الإستبانة المعلومات الخاصة بالفرد وخبرته فيما يخص موضوع أمن نظم المعلومات ويمكن توضيح نتائج الإجابات للعينة من خلال الجدول الآتي:

الجدول ٩
الفرد وخبرته فيما يخص أمن نظم المعلومات

ت	الاسئلة	محدودة		متوسطة		واسعة		الوسط الحسابي
		ت	%	ت	%	ت	%	
١	لدي قدرة على تطوير ونشر سياسات استخدام جيدة لأمن نظم المعلومات؟	١١	٢٠.٠٠	٣٥	٦٣.٤٦	١١	٢٠	٢.٠٣٦٤
٢	لدي قدرة على استخدام برامجيات تجعل أنظمة التشغيل أحدث مايمكن؟	٢٤	٤٣.٦٤	٢١	٣٨.١٨	٢٤	٤٣.٦٤	٢.٢٥٥
٣	لدي قدرة على وضع برامجيات تعمل على إعداد حواسيب قادرة على التحقق من هوية المستخدم؟	١٨	٣٢.٣٧	٢٣	٤١.٨٢	١٤	٢٥.٥٤	٢.٠٧٣
٤	لدي قدرة على السيطرة على عمليات إدخال البيانات إلى الأنظمة والآليات الخاصة بجمع البيانات؟	٢٩	٥٢.٧٣	١٣	٢٣.٦٤	١٣	٢٣.٦٤	٢.٢٩١
٥	لدي قدرة على على اتخاذ الإجراءات المناسبة لاكتشاف الأنشطة الشبكية والحاسوبية غير المخولة والمشبوهة؟	٩	١٦.٣٦	٢٩	٥٢.٧٣	١٩	٣٠.٩١	١.٨٥٤
٦	لدي قدرة على فحص الملفات والمجلدات لإيجاد اي تغييرات يمكن أن تتم على المعلومات المهمة فيها؟	١٧	٣٠.٩١	٢٦	٤٧.٢٧	١٢	٢١.٨٢	٢.٠٩٠
٧	لدي قدرة على مراقبة وفحص أنشطة النظام للبحث عن سلوكيات غيرمتوقعة يمكن أن تشكل خطراً على النظام؟	٢٣	٤١.٨٢	٢١	٣٨.١٨	١١	٢٠.٠٠	٢.٢١٨

ت	الاسئلة	محدودة		متوسطة		واسعة		الوسط الحسابي
		ت	%	ت	%	ت	%	
٨	لدي قدرة على مراقبة وفحص انشطة الشبكات المستند عليها النظام من إدراك السلوكيات غير المتوقعة والتي يمكن أن تشكل خطراً على النظام؟	١٣	٢٣.٦٤	٢٩	٥٢.٧٣	١٣	٢٣.٦٤	٢.٠٠
٩	لدي قدرة على جمع وحماية المعلومات ذات العلاقة بتهديدات معينة تعرض لها النظام وبالتالي الإستفادة منها في المستقبل؟	١٥	٢٧.٢٧	٢٦	٤٧.٢٧	١٤	٢٥.٤٥	٢.٠١٨
١٠	لدي قدرة على توفير آليات الدخول إلى جدران النار وآليات الحماية الأخرى البديلة عنها؟	١٥	٢٧.٢٧	٢٢	٤٠.٠٠	١٨	٣٢.٧٣	١.٩٤٥
	المتوسط العام							٢.٠٧٨٢

المصدر : من اعداد الباحثان بالاعتماد على نتائج الحاسوب.

يلاحظ من خلال الجدول أن المتوسط العام للإجابات بلغ ٢.٠٧٨٢ وهي نسبة تقترب من النسب الخاصة بالإجابات الإيجابية، أي إن معظم إجابات الأفراد تميل إلى الإيجاب أكثر منه للسلب فيما بخص الفرد وخبرته في مجال نظم المعلومات.

وقد تضمنت استمارة الاستبيان جزءاً خاصاً بالأسئلة ذات العلاقة بالمنظمة التي يعمل بها الأفراد المبحوثين ومدى توافر الإمكانيات المادية والبرامجية والبنية التحتية، فضلاً عن التشريعات القانونية، ويمكن توضيح نتائج الوصف الإحصائي لها من خلال الجدول الآتي:

الجدول ١٠

الجزء الخاص بالمنظمة التي يعمل بها الفرد ومدى توافر الإمكانيات اللازمة في المنظمة

ت	الاسئلة	نعم		لا		لا اعلم		الوسط الحسابي
		ت	%	ت	%	ت	%	
١	مدى امتلاك المنظمة التي يعمل الأفراد المبحوثين بها إطارعمل للسيطرة على تطبيق أمن نظم المعلومات.	٢٧	٤٩.٠٩	١٧	٣٠.٩١	١١	٢٠.٠٠	٢.٢٩١
٢	مدى امتلاك المنظمة التي يعمل بها الأفراد المبحوثين لإحصائية بكافة المعلومات المخزونة في قواعد البيانات والبرامجيات بالاضافة إلى الاصول المادية.	٣٤	٦١.٨٢	٩	١٦.٣٦	١٢	٢١.٨٢	٢.٤٠٠
٣	تمتلك المنظمة التي يعمل بها الفرد إمكانية تعزيز وتقوية مسؤوليات أمن نظم المعلومات بالنسبة للموظفين أثناء قيامهم بعملهم	٣١	٥٦.٣٦	١٣	٢٣.٦٤	١١	٢٠.٠٠	٢.٣٦٤
٤	تمتلك المنظمة التي تعمل بها إجراءات تبليغ رسمية خاصة باحتماليات الإختراقات الأمنية ومواضع الضعف في نظم المعلومات المحتمل استغلالها.	١٤	٢٥.٥٤	٢٤	٤٣.٦٤	١٧	٣٠.٩١	١.٩٤٥
٥	مدى امتلاك المنظمة التي يعمل بها الفرد لاجراءات توثيق وتبليغ رسمية لأي أعطال يمكن أن تحدث للبرامجيات	٣١	٥٦.٣٦	١٦	٢٩.٠٩	٨	١٤.٥٥	٢.٤١٨
٦	مدى امتلاك المنظمة التي يعمل بها الفرد لإجراءات خاصة بإدارة أي اختراقات أمنية لأمن نظم المعلومات	٢٠	٣٦.٣٦	٢٠	٣٦.٣٦	١٥	٢٧.٢٧	٢.٠٩١

ت	الاسئلة	نعم		لا		لا اعلم		الوسط الحسابي
		ت	%	ت	%	ت	%	
٧	مدى امتلاك المنظمة التي يعمل بها الفرد لسياسات رسمية تتطلب التوافق مع تراخيص البرامجيات.	١٢	٢١.٨٢	٢٦	٤٧.٢٧	١٧	٣٠.٩١	١.٠٩٠٩
٨	مدى امتلاك المنظمة لسياسات رسمية للحماية من الخطر المرتبط بالحصول على الملفات ذات العلاقة بعمل نظم المعلومات من مصادر غير موثوقة.	١٣	٢٣.٦٤	٢٣	٤١.٨٢	١٩	٣٤.٥٥	١.٨٩١
٩	مدى امتلاك المنظمة التي يعمل بها الفرد لبرامج فعالة لمكافحة الفيروسات مع التحديث المستمر عليها.	٤١	٧٤.٥٥	١١	٢٠.٠٠	٣	٥.٤٥	٢.٦٩٠٩
١٠	يوجد في المنظمة فحص لمرفقات البريد الالكتروني قبل فتحها لاحتمال وجود برامج تخريبية.	٢٣	٤١.٨٢	٢٣	٤١.٨٢	٩	١٦.٣٦	٢.٢٥٤٥
١١	مدى امتلاك المنظمة التي يعمل بها الفرد لنسخ احتياطية للمعلومات الأساسية والبرامجيات في قواعد مجدولة.	٣١	٥٦.٣٦	١٣	٢٣.٦٤	١١	٢٠.٠٠	٢.٣٦٤
١٢	مدى امتلاك المنظمة التي يعمل بها الفرد لسياسات دخول للمستخدمين لكل نظام وابسطها متطلبات كلمات المرور.	٤٠	٧٢.٧٣	١٢	٢١.٨٢	٣	٥.٤٥	٢.٦٧٦
١٣	تمتلك الأنظمة التي تعمل في المنظمة متطلبات اساسية تتضمن عدم خزن اية كلمات مرور لمستخدمين مخولين أثناء دخولهم إلى النظام لاحتمال استغلالها من قبل المخترقين.	٢٠	٣٦.٣٦	٢٣	٤١.٨٢	١٢	٢١.٨٢	٢.١٤٥
١٤	تمتلك المنظمة التي يعمل بها الفرد المبحوث سياسة مكتوبة لشروط الاستخدام الملائم للشبكة، والصلاحيات الخاصة بكل فرد والضوابط الادارية التي تعزز عملها.	٢٨	٥٠.٩١	١٥	٢٧.٢٧	١٢	٢١.٨٢	٢.٢٩١
١٥	تمتلك المنظمة التي يعمل بها الفرد متطلبات أساسية تتضمن عدم عرض رسائل مساعدة قبل الدخول إلى النظام لاحتمال استغلالها من قبل المخربين للدخول إلى النظام وإجراء تغييرات.	١٧	٣٠.٩١	٢١	٣٨.١٨	١٧	٣٠.٩١	٢.٠٠٠
١٦	يمتلك النظام الذي يعمل في المنظمة شرط عدم عرض أية رسائل تحذيرية يمكن أن تتضمن معلومات مفيدة لغير المخولين تساعدهم في الدخول إلى النظام.	١٨	٣٢.٧٣	٢٧	٤٩.٠٩	١٠	١٨.١٨	٢.١٤٥
١٧	تمتلك المنظمة التي يعمل بها الفرد إجراءات رقابية سواء للسجلات المنظمية، أو السجلات الخاصة بأمن نظم المعلومات.	١٣	٢٣.٦٤	٢٨	٥٠.٩١	١٤	٢٥.٥٤	٢.٩٨١٩
١٨	تمتلك المنظمة التي يعمل بها الفرد سياسات مطبقة للتأكد من توافقها مع قوانين حقوق النشر	٧	١٢.٧٣	٣٠	٥٤.٥٥	١٨	٣٢.٧٣	١.٨٠٠٠
	المتوسط العام							**٢.٢٥٨**

المصدر : من اعداد الباحثان بالاعتماد على نتائج الحاسوب.

ومن خلال تحليل الإجابات الخاصة بأفراد العينة للجزء الخاص بالمنظمة التي يعمل بها الفرد يلاحظ أن قيمة المتوسط العام بلغت 2.258، أي إن معظم الإجابات كانت إيجابية أكثر منها إلى السلب.

٢- تحليل التباين لعينة الدراسة

تم إجراء تحليل التباين لإجابات عينة الدراسة، وتم تقسيم هذا التحليل على قسمين، الأول تحليل التباين في إجابات العينة فيما يخص مستوياتها كالجنس والعمر والخبرة العملية المباشرة والتدريب والتأهيل، وعدد الساعات الأسبوعية التي يقضيها في العمل المرتبط بنظم المعلومات، وعدد سنوات الخدمة وملاحظة اختلاف الإجابات ما بينها وما بين القسم الأول من الأسئلة والخاص بالفرد وخبرته في مجال نظم المعلومات والجدول الآتي يوضح تحليل التباين One-way ANOVA، لكل مستوى من المستويات في مقابل إجابات العينة فيما يخص المعلومات الخاصة بالفرد وخبرته في مجال نظم المعلومات.

الجدول ١١
تحليل التباين لمستويات العينة بالمقارنة مع إجابات الأسئلة الخاصة بالفرد وخبرته في مجال نظم المعلومات

تحليل التباين / المستويات	F		DF	
	الجدولية	المحسوبة	المقام	البسط
الجنس	٤.٠٤	٦.٢٤	١	٥٣
الفئة العمرية	٢.٥٧	١.٢٥	٤	٥٠
الخبرة العملية المباشرة	٣.١٩	٣.٩٥	٢	٥٢
التدريب والتأهيل	٤.٠٤	٣.٢٨	١	٥٣
عدد السنوات الأسبوعية التي يقضيها في العمل المرتبط بنظم المعلومات	٢.٤١	٠.٥٦	٥	٤٩
عدد السنوات الخدمة	٢.٤١	١.٠٨	٥	٤٩

المصدر : من اعداد الباحثان بالاعتماد على نتائج الحاسوب.

١. تحليل التباين من حيث الجنس: نلاحظ من خلال الجدول أن قيمة F المحسوبة ٦.٢٤ وهي أكبر من القيمة الجدولية البالغة ٤.٠٤، وذلك عند مستوى معنوية ٠.٠٥ وبدرجات حرية (١، ٥٣)، وهذا يقودنا إلى رفض الفرضية الثانية وقبول البديلة، أي يوجد تباين ما بين إجابات عينة البحث بالنسبة للذكور والإناث فيما يخص المعلومات الشخصية والخبرة في مجال نظم المعلومات.
٢. تحليل التباين من حيث الخبرة العملية المباشرة: نلاحظ أيضاً من خلال الجدول أن قيمة F المحسوبة ٣.٩٥ وهي أكبر من القيمة الجدولية البالغة ٣.١٩ عند مستوى معنوية ٠.٠٥ وبدرجات حرية (٢، ٥٣)، وهذا يقودنا إلى رفض الفرضية الثالثة وقبول البديلة، أي إنه يوجد تباين ما بين آراء عينة البحث ذوي الخبرة المحدودة أو المتوسطة أو الواسعة فيما يخص المعلومات الشخصية والخبرة في مجال نظم المعلومات.
٣. تحليل التباين من حيث التدريب والتأهيل: ويلاحظ من خلال الجدول أن قيمة F المحسوبة بلغت ٣.٢٨ وهي أقل من القيمة الجدولية البالغة ٤.٠٤ عند مستوى معنوية ٠.٠٥ وبدرجات حرية (١، ٥٣)، وهذا يقودنا إلى قبول الفرضية الأولى، أي إنه لا يوجد تباين ما بين إجابات عينة البحث للمتدربين وغير المتدربين فيما يخص المعلومات الشخصية والخبرة في مجال أمن نظم المعلومات.

وفيما يتعلق بالجزء الثاني أي الأسئلة الخاصة بالمنظمة التي يعمل بها الفرد والإمكانيات المتوافرة والبنية التحتية المادية والبرمجية والتشريعية للمنظمة ومقارنة تباين إجابات العينة بين مستوياتها المختلفة كالفئة العمرية والجنس والتدريب والتأهيل وغيرها من المستويات، فيمكن توضيح التباينات من خلال الجدول الآتي:

الجدول ١٢
تحليل التباين بالمقارنة مع إجابات الأسئلة الخاصة بالمنظمة التي يعمل بها الفرد

تحليل التباين / المستويات	F		DF	
	الجدولية	المحسوبة	المقام	البسط
الجنس	٤.٠٤	٠.٤٣	١	٥٣
الفئة العمرية	٢.٥٧	٠.٧٧	٤	٥٠
الخبرة العملية المباشرة	٣.١٩	٠.٦٩	٢	٥٢
التدريب والتأهيل	٤.٠٤	٠.٦٤	١	٥٣
عدد السنوات الأسبوعية التي يقضيها في العمل المرتبط بنظم المعلومات	٢.٤١	٢.١٨	٥	٤٩
عدد السنوات الخدمة	٢.٤١	٠.٥٨	٥	٤٩

المصدر : من اعداد الباحثان بالاعتماد على نتائج الحاسوب.

١. تحليل التباين من حيث الجنس: نلاحظ من خلال الجدول أن قيمة F المحسوبة بلغت ٠.٤٣ وهي أقل من القيمة الجدولية البالغة ٤.٠٤ وذلك عند مستوى معنوية ٠.٠٥ وبدرجتي حرية (١، ٥٣) وهذا يقودنا إلى قبول الفرضية الثانية، أي لايوجد تباين ما بين إجابات عينة البحث بالنسبة للذكور والإناث فيما يخص المنظمة ومدى توافر الإمكانيات المادية والبرمجية والتشريعات القانونية التي تدعم عملها.
٢. تحليل التباين من حيث الخبرة العملية المباشرة: نلاحظ أيضاً من خلال الجدول أن قيمة F المحسوبة ٠.٦٩ وهي أقل من القيمة الجدولية البالغة ٣.١٩ عند مستوى معنوية ٠.٠٥ وبدرجتي حرية (٢، ٥٢)، وهذا ما يقودنا إلى قبول الفرضية الثالثة، أي إنه لا يوجد تباين ما بين آراء عينة البحث ذوي الخبرة المحدودة أو المتوسطة أو الواسعة فيما يخص المنظمة ومدى توافر الإمكانيات المادية والبرمجية والتشريعات القانونية التي تدعم عملها.
٣. تحليل التباين من حيث التدريب والتأهيل: ويلاحظ من خلال الجدول أن قيمة F المحسوبة بلغت ٠.٦٤ وهي أقل من القيمة الجدولية البالغة ٤.٠٤ عند مستوى معنوية ٠.٠٥ وبدرجتي حرية (١ ،٥٣)، وهذا يقودنا إلى قبول الفرضية الأولى، أي إنه لايوجد تباين مابين إجابات عينة البحث للمتدربين وغير المتدربين فيما يخص المنظمة ومدى توافر الإمكانيات المادية والبرمجية والتشريعات القانونية التي تدعم عملها.

الاستنتاجات والتوصيات

أظهرت نتائج هذه الدراسة عدم تباين إجابات أفراد عينة الدراسة من المتدربين وغير المتدربين وهذا يدل على عدم فاعلية البرامج التدريبية التي يحصلون عليها فيما

يخص موضوع أمن المعلومات بشكل عام و أمن نظم المعلومات بشكل خاص، وهذا يمكن تحديده من خلال قيمة F المحسوبة والتي بلغت ٠.٦٤ وهي أصغر من القيمة الجدولية البالغة ٤.٠٤، أي إنها غير معنوية، وبالتالي سنقبل فرضية العدم ونرفض البديلة، مما يدل على أن المعلومات التي حصلوا عليها، إما من خلال معلوماتهم وقراءاتهم الشخصية، أو من خلال سنوات الخبرة التي حصلوا عليها عملهم، وبناءً على النتائج المذكورة يوصي الباحثان بما يأتي:

١. ضرورة توفير برامج تدريبية متخصصة بأمن نظم المعلومات للأفراد الذين يرتبط عملهم المباشر بأمن نظم المعلومات.
٢. ضرورة توفير بنى تحتية وإمكانيات وتشريعات قانونية تدعم تطبيق المعلومات التي يحصل عليها المتدربين من البرامج التدريبية في أرض الواقع.
٣. ضرورة تشخيص نقاط الضعف في أنظمة المعلومات لغرض تحديد الأدوات والتقانات الضرورية لتلافي العيوب في النظام وحمايته من أي تهديدات أو مخاطر.
٤. ضرورة التركيز بشكل أكبر على أمن نظم المعلومات بوصفه من المواضيع المهمة التي يعتمد عليها في تحقيق أمن وحماية نظم المعلومات من المخاطر المحتملة سواءً من داخل المنظمة أو من خارجها.
٥. لابد من توفير أنظمة تتمتع بامكانيات أفراد متدربين قادرين على حماية المكونات المادية كجدران النار، أو استخدام كلمات المرور، والبرامجيات كمضادات الفيروسات الفعالة.

المراجع

أولاً- المراجع باللغة العربية

١. بيل، مالكوم، ١٩٩٧، التدريب الناجح للموظفين، الدار العربية للعلوم، الطبقة الأولى.
٢. السكارنة، بلال خلف، ٢٠٠٩، التدريب الاداري، دار الوائل للنشر، الطبعة الأولى.
٣. العمري، خالد، ٢٠٠٧، الخطوات السبع للتدريب الفعال، دار الفاروق للاستثمارات الثقافية، مصر.
٤. نينو، ماركو ابراهيم ، الحميد، دباس حميد، حماية انظمة المعلومات، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان الاردن.
٥. ياسين، سعد غالب، ٢٠٠٨، نظم المعلومات الادراية، دار اليازوي العلمية للنشر والتوزيع، عمان الاردن .

ثانياً- المراجع باللغة الاجنبية

1. Anderson, Jacobson,2008, "Privacy and Security in Internet-Based Information Systems", Dissertation, Blekinge Institute of Technology, Department of Systems and Software Engineering, School of Engineering, Sweden. (http://www.bth.se/fou/forskinfo.nsf/6753b78eb2944e0ac1256608004f0535/f26dd7141e165324c12573f6002db90c/$file/Jacobsson_diss.pdf).
2. Baral, Hemanta Raj, 2010, "A Protocol for Network Security Assessment Methodology", Dissertation, Angela Ruskin University Chelmsford,UK. (http://www.hemantabaral.com/Dissertation.pdf).
3. Bener, Ayse Basar, 2000, "Risk Perception, 3- Trust and Credibility, A Case in Internet Banking", Dissertation, London School of Economics and Political Sciences. (http://csrc.lse.ac.uk/research/theses/bener.pdf).

4. Braynt, Adam R., 2007, "Developing a Framework for Evaluating Organizational Information- Assurance Metrics Programs", Master thesis, Faculty Department of Systems and Engineering Management, Graduate School of Engineering and Management ,Air Force Institute of Technology, Air University. (http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA467367).
5. Dhillon, 1995, " Interpreting the Management of Information Systems Security", Dissertation, Department of Information Systems, London School of Economics and Political Science, University of London, UK. (http://60.88.dyn.lse.ac.uk/research/theses/dhillon.pdf).
6. Dhillon, Gurpreet,2007, "Princeples of Information Systems Security- Text and Cases", Willey andSons, .Inc, USA.
7. Farahmand, Fariborz, 2004," Developing a Risk Management System for Information Systems Security Incidents", Dissertation, College of Computing Georgia Institute of Technology. (https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/Farahmand.pdf)
8. Hutchison, 2011, "Computer Network Security", Third International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security,MMM-ACNS 2005, St. Petersburg, Russia, (Stewart et.al, 2011 , CISSP, (Certified Information Systems), Security Professional, Study Guide, Fifth Edition, Wiley Publishing .INC., Indianapolis, Indiana, USA.
9. Jessup, Leonardand, Valanch, Joseph, "Information Systems Today- Managing the Digital World", Pearson Prentice Hall, Inc.
10. Kreicberga, Liene, 2010, "Internal Threat to Information Security, Countermeasure and Human Factor Within, SME", Master Thesis, Department of Business Administration and Social Sciences, Division of Information Systems Sciences,Lulea University of Technology. (http://epubl.ltu.se/1653-0187/2010/050/LTU-PB-EX-10050-SE.pdf).
11. Laundon and Laundon, 2002, "Mangement Information Systems- Managing The Digital Firm" , Seventh Edition, prentice –Hall.Inc,New Jersey, USA.
12. Laundon and Laundon, 2009, "Essentials of Management Information Systems", Eighth Edition, Pearson Education, Inc, New Jersey, USA.
13. Laundon and Laundon, 2010, "Manangement Information Systems- Mangeing the Digital Firm", Eleventh Edition, Global Edition, Pearson Education, Inc, New Jersey, USA.
14. Matthew K.Burnburg,2003, "A Proposed Framework for Business Information Security Based on the Concept of Defence -In-Depth ", Master Thesis, School of Business and Management, University of Illinois. (http://mis2.uis.edu/projects/MBurnburg.pdf).
15. Miller and Gregg, 2007, "Security Administrator Street Smarts, A Real World Guide to CompTIA Security+ Skills", Wiley Publishing, Inc., Indianapolis, Indiana., Canada.
16. Mislove, Alan E., 2009, "Online Social Networks: Measurement, Analysis, and Applications to Distributed Information Systems", PHD thesis, Rice University, Houston,Texas. (http://www.ccs.neu.edu/home/amislove/publications/SocialNetworks-Thesis.pdf).
17. Nachtigal, Sharon, 2009, "E-business Information Systems Security Design Paradigm and Model", Technical Report, Department of Mathematics, Royal Holloway, University of London Egham, Surrey TW20 0EX, England. (http://www.ma.rhul.ac.uk/static/techrep/2009/RHUL-MA-2009-16.pdf).
18. Nakrem, Are, 2007, "Managing Information Security in Organizations , a Case study", Master Thesis, Institute of Information Science, Department of Economy and Social Science Studies, HIS, Agder University Collage.

(http://brage.bibsys.no/hia/bitstream/URN:NBN:nobibsys_brage_2540/1/master_infosys_2007_nakrem.pdf).

19. Nampanda, Kondwani, 2012, 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.
(http://pure.ltu.se/portal/files/36200540/LTU-EX-2012-36196156.pdf).
20. Oscarson, Per, 2007, "Actual and Perceived Information Systems Security" Dissertation, Department of Management and Engineering, Linköping University, Linköping, Sweden.
(http://Lio.diva-portal.org).
21. Phelpes, 2005, "Information System Security: Self – Efficacy and Security Effectiveness in Florida Libraries", Dissertation, College of Information, The Florida State University.
(http://etd.lib.fsu.edu/theses/available/etd-02082005-035903/unrestricted/dissertation.pdf).
22. Puhakainen, Petri, 2006, " A Design Theory for Information Security Awareness", Dissertation, Faculty of Science, Department of Information Processing Science, University of Oulu.
(http://herkules.oulu.fi/isbn9514281144/isbn9514281144.pdf).
23. Schuessler, Joseph H., 2009, "General Deterrence Theory: Assessing Information Systems Security Effectiveness in Large Versus Small Businesses", Dissertation, University of North Texas.
(http://nsl.cse.unt.edu/~dantu/cae/attachments/JosepthSchuesslerDissertation.pdf).
24. Stair, Ralph and, Reynold, George,2010, "Information Systems", Ninth Edition, Canada.
25. Stewart *et.al.*, 2009, "CISSP-Certified Information Systems Security-Study Guide", Fifth Edition, Willey Publishing, Inc., Indianapolis, Indiana, USA.
26. Stjerneby, Anna, 2002, Identification of Security Relevant Characteristics in Distributed Information Systems, Master Thesis, Avdelning, Institution ,Division, Department, Linkopings University, Sweden .
(http://liu.diva-portal.org).
27. Stojaković-, Suzana, 2000, "Building Secure Information Systems ",Faculty of Electrical. Engineering, Department of Computer Science and Engineering, Czech Technical University in Prague.
(http://agn-www.informatik.uni-hamburg.de/papers/doc/diss_suzanza_stojakovic-celustka.pdf).
28. Williams, Paul D., 2005, "Cupids Increasing Information System Through The Use of Dedicated Co-Processing", Purdue University .
(http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA440440).
29. Wu, Xianping, 2009, "Security Architecture for Sensitive Information Systems", Phd Thesis, Faculty of Information Technology, Monash University, Australia.
(http://www.csse.monash.edu.au/~srini/theses/Ping_Thesis.pdf).
30. Zissis, Dimitrios, 2011, Methodologies and Technologies for Designing Secure Electronic Voting Information Systems, Dissertation, Department of Product and Systems Design Engineering, University of the Aegean.
(http://www.syros.aegean.gr/documents/phd/phd_dzissis.pdf).