أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات - دراسة ميدانية في شركات الاتصالات العاملة في اليمن

أ.د. محمد علي الربيدي[1]
أ. نبيل حسان عبده الحميري[2,*]

الاستلام: 11/فبراير/2021
التحكيم: 20/فبراير/2021
القبول: 25/مارس/2021

[1] أستاذ المحاسبة، جامعة العلوم والتكنولوجيا، اليمن
[2] مدرس المحاسبة المساعد، جامعة العلوم والتكنولوجيا، اليمن
*عنوان المراسلة: nabelal2000@yahoo.com

https://doi.org/10.20428/JSS.27.1.5

أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات - دراسة ميدانية في شركات الاتصالات العاملة في اليمن

الملخص:

هدفت الدراسة إلى قياس أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات بالاعتماد على نمذجة المعادلة البنائية (SEM) كدراسة تحليلية، ويتمثل مجتمع الدراسة في شركات الاتصالات العاملة في اليمن البالغ عددها 7 شركات، وتم استخدام الاستبانة أداةً لجمع البيانات من 356 مشاركا، وقد وصل عدد الاستبانات الصالحة للتحليل 218 استبانة، وتم معالجة البيانات باستخدام طريقة المربعات الصغرى الجزئية (PLS). وقد توصلت الدراسة إلى أن مخاطر تكنولوجيا المعلومات تؤثر سلبا في أمن نظم المعلومات. وأوصت الدراسة بضرورة تعزيز أمن نظم المعلومات للحفاظ على سرية المعلومات وسلامتها وتوافرها من المخاطر، ومواكبة أمن المعلومات للتطورات المتسارعة في تكنولوجيا المعلومات والاتصالات.

الكلمات المفتاحية: أمن نظم المعلومات، شركات الاتصالات العاملة في اليمن، مخاطر تكنولوجيا المعلومات.

https://doi.org/10.20428/JSS.27.1.5

Impact of Information Technology Risks on Information Systems Security: A Field Study of Telecommunication Companies in Yemen

Abstract:

This study aimed to assess the impact of information technology risks on security of information systems by following an analytical method based on the structural equation modeling (SEM). The study population was seven telecommunication companies in Yemen. A questionnaire was distributed to 356 participants, but only 218 forms were valid for analysis. The data was analyzed by the partial least squares (PLS). The study findings revealed that information technology risks had a negative impact on the security of information systems. The study recommended that the security of information systems should be strengthened so as to maintain the confidentiality of information, its availability and integrity from risks, and to cope with speedy developments in information and communication technology.

Keywords: information systems security, telecommunication companies in Yemen, information technology risks.

https://doi.org/10.20428/JSS.27.1.5

المقدمة:

يُعد أمن المعلومات في مقدمة أولويات واهتمامات الأفراد والمنظمات والدول؛ حيث أشار تقرير الأمن السيبراني (Cisco, 2015, 48) إلى أن ثلثي المستجيبين أفادوا أن القيادة التنفيذية في منظماتهم تعتبر الأمن أولوية عالية. ووجدت دراسة جرائم وأمن الحاسوب (Richardson, 2010, 32) أن نصف المستجيبين يرون أن الإدارة العليا تعتبر الأمن من أولوياتها العالية، وكذلك قضايا أمن المعلومات تحتل مساحة واسعة من الدراسات والأبحاث وعقد المؤتمرات، فقد أكدت العديد من الدراسات أن أولوية أمن المعلومات وأهميتها عالية في منظمات الأعمال وفي مقدمة أولوياتهم تأمين بيئة تكنولوجيا المعلومات (AICPA, 2015, 13; Ernst &Young, 2012,15; PwC, 2014, 4).

وقد أدى انتشار الأنظمة وشبكات المعلومات والاعتماد عليها إلى عدم قدرة أي نشاط تجاري إهمال القضية الأمنية (Riad, 2009, 35)؛ حيث أتاح استخدام تكنولوجيا المعلومات والاتصالات ونظم المعلومات إمكانيات وفرص كبيرة لخدمة المنظمة (زويلف، 2009، 48)، وأسهم استخدام التكنولوجيا في رفع القدرات التحليلية، ورفع كفاءة أنشطة المنظمة، وإنجاز العمليات بدقة وسرعة عالية (Bafghi, 2014, 75)، وتحقيق نمو كبير في إجراء المعاملات وتقديم الخدمات عبر الإنترنت (Brown, DeHayes, Hoffer, Martin, & Perkins, 2012, 561). ورافق استخدام تكنولوجيا المعلومات والاتصالات وتطورها العديد من المخاطر التي تؤثر في أمن نظم المعلومات (Jouini, Rabai, & Aissa, 2014, 489)، فقد عانت منظمات الأعمال من العديد من المخاطر التي تستهدف سرية وسلامة وتوافر المعلومات المتمثلة في الهجمات الإلكترونية والمادية، والبرامج الخبيثة، وإخفاق الأجهزة، وأخطاء البرامج، وكوارث طبيعية وغير طبيعية (Joint Task Force Transformation Initiative, 2012, 8). وقد تؤدي هذه الهجمات إلى فقدان السرية، أو فقدان السلامة، أو فقدان التوافر، أو فقدان عنصرين أو أكثر (Donaldson, Siegel, Williams, & Aslam, 2015, 10). والآثار السلبية المحتملة في حال فقدان عناصر أمن المعلومات إما أن تكون محدودة، أو خطيرة، أو شديدة الخطورة (كارثية) على عمليات وأصول المنظمة (Government Accountability Office, 2016a, 6).

وقد تناول العديد من الباحثين قضايا أمن نظم المعلومات على نطاق واسع ومن جوانب مختلفة، حيث أشار البعض إلى أن المخاطر في شركات الاتصالات تزداد باستمرار من حيث الكم والنوع والتأثير (Deloitte, 2006, 3; Deloitte, 2014, 16). ورصدت العديد من الدراسات والتقارير اختراق أنظمة المعلومات (Deloitte, 2016, 3; Department for Culture Media and Sport, 2016)، وناقش الباحثون الآثار السلبية الناجمة عن الاختراقات الأمنية والمتمثلة في الخسائر المالية، وإلحاق أضرار بسمعة الشركة، والعلامة التجارية، وتوقف النظام، وفقدان إيرادات (Deloitte, 2006, 3)، وأكد تقرير (Deloitte, 2014, 16) أن الهجمات التي استهدفت شركات الاتصالات أدت إلى إلحاق أضرار كبيرة بسمعة الشركات وسرية المعلومات وأثارت مخاوف العملاء المتعلقة بالخصوصية، وفقدان الثقة.

وبالتالي لا توجد بيئة تقنية آمنة بنسبة 100 %، وكل بيئة يوجد بها نقاط ضعف وأوضاع عُرضه للإصابة وتهديدات إلى درجة معينة، وأن الصراع مستمر بين أمن المعلومات والمخاطر، وأمن المعلومات عملية لا تنتهي ولا تتوقف عند حد معين، طالما استمرت تكنولوجيا المعلومات في تطور متصاعد (القحطاني، 2015)؛ لذلك تم دراسة أمن المعلومات لتحقيق هدف الدراسة الحالية المتمثل في قياس أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات في شركات الاتصالات العاملة في اليمن.

أمن نظم المعلومات:

مع تزايد اعتماد الشركات على نظم المعلومات المحوسبة تصبح قضية أمن النظام مسألة ذات أهمية قصوى (Arsenie-Samoil, 2011, 1344)، حيث يقوم أمن المعلومات بأداء أربع وظائف مهمة، وهي: 1) حماية قدرة المنظمة على العمل. 2) التشغيل الآمن للتطبيقات. 3) حماية البيانات. 4) حماية الأصول التقنية المستخدمة في المنظمة (Whitman & Mattord, 2011, 41).

مفهوم أمن نظم المعلومات:

استندت بعض تعريفات أمن المعلومات إلى مجموعة من العناصر الأمنية التي يجب تحقيقها (كالسرية، والسلامة، والتوافر، والموثوقية، وعدم الإنكار، والمصادقة، والتخويل)، والتناقض بين التعريفات هو أن بعضها ترى أن المعلومات آمنة إذا كانت محمية من جميع المخاطر، بينما تشير التعريفات الأخرى إلى أن المعلومات آمنة إذا تحققت بعض العناصر الأمنية (ربط الأمن بمجموعة من العناصر الأمنية)، وعلى الرغم من اختلاف مجموعة العناصر الأمنية المرتبطة بأمن المعلومات، فإنها تتفق على العناصر الأساسية لأمن المعلومات، وهي: السرية والسلامة والتوافر (Cherdantseva & Hilton, 2015, 8). ويُقصد بأمن المعلومات حماية المعلومات من مجموعة واسعة من المخاطر من أجل ضمان استمرارية الأعمال، وخفض مخاطر الأعمال، وتعظيم العائد على الاستثمار (International Organization for Standardization (ISO), 2010, 59). وعرّفت لجنة أنظمة الأمن القومي (Committee on National Security Systems, 2015, 66) مصطلح أمن نظم المعلومات بأنه: "حماية أنظمة المعلومات ضد الوصول غير المصرح به، أو تعديل المعلومات سواء عند التخزين أو المعالجة أو النقل، أو انقطاع الخدمة عن المستخدمين المخولين، بما في ذلك التدابير اللازمة للكشف عن المخاطر وتوثيقها ومواجهتها".

ولأغراض الدراسة الحالية فإنه يمكن تعريف أمن نظم المعلومات بأنه: حماية أنظمة المعلومات من مجموعة واسعة من المخاطر لضمان سرية المعلومات، وسلامتها، وتوافرها أثناء المعالجة أو التخزين أو النقل.

أهمية أمن نظم المعلومات:

أصبح أمن المعلومات مصدر قلق في جميع منظمات الأعمال والتحدي الأكبر لها (Riad, 2009, 35). وكما ذكر تقرير اتجاهات الأمن السيبراني أن خبراء الأمن السيبراني هم الأكثر قلقا بشأن هجمات الاصطياد الإلكتروني والبرامج الضارة (Wallis, 2018)، ونظرا لأهمية الأمن فقد استثمرت العديد من الشركات في مجال أمن المعلومات وتطبيقات الأعمال التجارية (Brown et al., 2012, 32)؛ لضمان سرية المعلومات، وسلامتها، وتوافرها في جميع مراحل دورة حياة المعلومات واستخدامها داخل الشركة (Joint Task Force Transformation Initiative, 2013, 1). وتتمثل أهمية أمن نظم المعلومات في تأمين المعلومات الحساسة من المخاطر من خلال برامج التوعية والتدريب، وتطبيق السياسة الأمنية، والمصادقة، والتحكم بالوصول، والتشفير، وقد أولت الهيئات المهنية قدرا كبيرا من الاهتمام بالمعايير والسياسات والقوانين واللوائح وتطويرها لمساعدة منظمات الأعمال على تأمين معلوماتها بشكل كافٍ من المخاطر (AlKalbani, Deng, Kam, & Zhang, 2017, 104).

وتؤكد العديد من الدراسات على أهمية أمن المعلومات في منظمات الأعمال؛ حيث أشارت الدراسات (Cisco, 2015, 48; Ernst & Young, 2015; PwC, 2014, 4; Richardson, 2010, 32) إلى أن الإدارة العليا والقيادة التنفيذية في منظمات الأعمال تعتبر الأمن أولوية عالية وفي مقدمة اهتماماتهم.

أبعاد أمن نظم المعلومات:

أمن نظم المعلومات هو الحفاظ على سرية المعلومات، وسلامتها، وتوافرها؛ وذلك وفقا لتعريف المنظمة الدولية للمعايير (ISO, 2018, 4)، والمعهد الوطني للمعايير والتكنولوجيا (Paulsen & Toth, 2016, 2)، ووفقا لذلك يتضمن التعريف حماية المعلومات ونظم المعلومات من الوصول غير المصرح به، أو الاستخدام، أو الكشف، أو التعديل، أو الإتلاف، أو التوقف من أجل ضمان السرية، والسلامة، والتوافر (Committee on National Security Systems, 2015, 94). ويتم قياس أمن نظم المعلومات من خلال الأبعاد الثلاثة: السرية، والسلامة، والتوافر التي تضمنها التعريف، وتوضيحها كالآتي:

(1) السرية هي حماية المعلومات من الكشف والوصول غير المصرح به (Paulsen & Toth, 2016, 2; ISO, 2018, 2). وتعتبر سرية المعلومات قضية جوهرية في قطاع الاتصالات؛ نظرا لاستخدامها على

https://doi.org/10.20428/JSS.27.1.5

نطاق واسع في التواصل وتخزين كميات كبيرة من البيانات الحساسة، وتؤدي هجمات التنصت والوصول غير المصرح به والاصطياد الإلكتروني والهندسة الاجتماعية إلى إلحاق أضرار كبيرة بالسمعة وإثارة مخاوف العملاء المتعلقة بالخصوصية، وبالتالي فقدان الثقة (Deloitte, 2014, 16).

(2) السلامة هي حماية المعلومات من التعديل والإتلاف غير المصرح به (Paulsen & Toth, 2016, 2). ويهتم هذا العنصر بدقة وسلامة المعلومات والأنظمة من التلاعب أو التعديل غير المصرح به، وكذلك يهتم بكشف تعديل المعلومات (القحطاني، 2015). وتعتمد سلامة المعلومات وتكاملها على الأجهزة والبرامج المستخدمة في تبادل المعلومات، ومعالجتها، وتخزينها (ISO, 2011, 40)، وتتحقق السلامة عندما تبقى البيانات دون تعديل من وقت إدخالها إلى النظام وحتى استرجاعها لاحقا (Donaldson et al., 2015).

(3) التوافر يعني ضمان إمكانية الوصول إلى الأنظمة والمعلومات في الوقت المناسب وإمكانية الاعتماد عليها واستخدامها (Kissel, 2013, 17; ISO, 2018, 2). ويهدف عنصر التوافر إلى أن تبقى أنظمة المعلومات متاحة للمخولين في جميع الأوقات مما يحول دون انقطاع الخدمة الناتج عن إخفاق الأجهزة، أو تحديث النظام، أو انقطاع الطاقة، أو هجمات الحرمان من الخدمة (Feruza & Kim, 2007, 19). وضمان التوافر يشمل استمرار العمليات، وإمكانية الوصول إلى البيانات، وسهولة استخدامها من قبل الأطراف المصرح لها في أي وقت وفي أي مكان (Seno, Bidmeshk, & Ghaffari, 2015, 3).

مخاطر تكنولوجيا المعلومات:

تحدث مخاطر أمن المعلومات بسبب التهديدات الأمنية المحتملة التي قد تستغل الثغرات الموجودة في أصل أو مجموعة من الأصول تؤدي إلى حدوث أضرار في المنظمة (ISO, 2014). ويعتمد تنفيذ الهجوم الإلكتروني على وجود دافع، وخطة واضحة لطريقة الهجوم، ووجود ثغرات في تصميم النظم والبرمجيات أو الأجهزة والشبكات (الغثبر والقحطاني، 2009). وأحد القضايا المهمة التي تعاني منها منظمات الأعمال حاليا هو استمرار ظهور مخاطر جديدة لم تشهدها المنظمات من قبل، وتتمثل الأضرار المترتبة على حدوث المخاطر في كشف المعلومات، أو تعديلها، أو إتلافها، أو الحرمان من الخدمة (Joint Task Force Transformation Initiative, 2012, 8)، وتتراوح الأضرار بين خسائر بسيطة إلى تدمير نظام بالكامل (Jouini et al., 2014, 489).

مفهوم مخاطر تكنولوجيا المعلومات:

عرّف المعهد الوطني للمعايير والتكنولوجيا مخاطر أمن المعلومات بأنها تلك المخاطر التي تنشأ عن فقدان سرية، أو سلامة، أو توافر المعلومات ونظم المعلومات وتنعكس الآثار السلبية المحتملة على عمليات وأصول المنظمة (Joint Task Force Transformation Initiative, 2012, 6). وعرّف مخاطر تكنولوجيا المعلومات بأنها الأثر المحتمل على الأعمال من مصدر تهديد معين يستغل ثغرات معينة في تكنولوجيا المعلومات (Joint Task Force Transformation Initiative, 2001, 18). وتنشأ مخاطر تكنولوجيا المعلومات عن: 1) كشف المعلومات غير المصرح بها، أو تعديلها، أو إتلافها. 2) الأخطاء أو الإهمال. 3) تعطل تكنولوجيا المعلومات بسبب الكوارث الطبيعية وكوارث من صنع الإنسان (Joint Task Force Transformation Initiative, 2001, 21).

ولأغراض الدراسة الحالية فإنه يمكن تعريف مخاطر تكنولوجيا المعلومات بأنها: الكشف غير المصرح به للمعلومات (فقدان السرية)، أو تعديل المعلومات أو إتلافها (فقدان السلامة)، أو تعطل أو توقف النظام والخدمات (فقدان التوافر)، ومن المحتمل أن تؤثر سلبا على عمليات وأصول المنظمة.

أبعاد مخاطر تكنولوجيا المعلومات:

مخاطر تكنولوجيا المعلومات هي تلك المخاطر التي تنشأ عن فقدان سرية، أو فقدان سلامة، أو فقدان توافر المعلومات ونظم المعلومات، وذلك وفقا للمعهد الوطني للمعايير والتكنولوجيا (Joint Task Force Transformation Initiative, 2012, 6)، ودراسة Azees، Vijayakumar وDeborah (2016)،

ودراسة Gordon، Loeb وZhou (2011، 33). ويتم قياس مخاطر تكنولوجيا المعلومات من خلال الأبعاد الآتية: (1) المخاطر المتعلقة بالسرية وتعني الكشف أو الوصول غير المصرح به للمعلومات السرية من خلال التنصت وكسر كلمة المرور، والوصول غير المصرح به، والأفعال المتعمدة، والاصطياد الإلكتروني والاجتماعي (Gordon et al., 2011, 35). (2) المخاطر المتعلقة بالسلامة وتعني التعديل أو الإتلاف غير المصرح به للمعلومات أو نظم المعلومات من خلال أفعال الموظفين، وأخطاء البرمجيات، والتقادم التكنولوجي (Ahmadzadegan, Elmusrati, & Mohammadi, 2013, 633; Rhodes-Ousley, 2013, 266). (3) المخاطر المتعلقة بالتوافر وتعني منع المستخدمين المخولين من الوصول إلى المعلومات أو نظام المعلومات عند الطلب من خلال هجمات الحرمان من الخدمة، والكوارث الطبيعية، وأعطال الأجهزة الفنية (Gordon et al., 2011, 35; Rhodes-Ousley, 2013, 267). وتم إضافة المخاطر العامة كبُعد جديد لمعالجة مشكلة ظهور بعض المخاطر في أكثر من بُعد، حيث تم تخصيص بُعد للمخاطر التي تستهدف السرية، وبُعد للمخاطر التي تستهدف السلامة، وبُعد للمخاطر التي تستهدف التوافر، وبُعد للمخاطر التي تستهدف عنصرين أو أكثر من عناصر أمن المعلومات (السرية والسلامة والتوافر) في آن واحد، مثل البرامج الضارة، والانتحال، وقرصنة الهاتف، وقد تؤدي هذه المخاطر إلى فقدان سرية المعلومات وسلامتها وتوافرها.

الدراسات السابقة:

ناقشت بعض الدراسات أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات، وتشير أغلب هذه الدراسات إلى وجود أثر سلبي، حيث أكدت دراسة Straub وWelke (1998) أن المخاطر تؤثر في أنظمة المعلومات. وأشارت دراسة Gordon et al. (2011)، Cavusoglu، Mishra وRaghunathan (2004)، ودراسة Ishiguro، Tanaka، Matsuura وMurase (2006) إلى أن اختراق أمن المعلومات يؤثر سلبا على عائدات الشركات. وذكرت دراسة Riad (2009) أن المخاطر تؤثر سلبا في أمن المعلومات. غير أن دراسة Campbell، Gordon، Loeb وZhou (2003)، ودراسة Kannan، Rees وSridhar (2007)، وجدت أن اختراق أمن المعلومات لا يؤثر على عائدات الشركات.

وفيما يتعلق بأثر مخاطر السرية في أمن نظم المعلومات، فقد أشارت دراسة Gordon et al. (2011)، ودراسة Ishiguro et al. (2006) إلى أن اختراق السرية يؤثر سلبا على عائدات الشركات في سوق الأوراق المالية. ووجدت دراسة Campbell et al. (2003) أن الوصول غير المصرح به للمعلومات السرية يؤثر سلبا على عائدات الشركات. وأكد تقرير Trend Micro (2015) أن 60 % من نقاط الضعف (مثل جوانب القصور في تنفيذ آليات التحقق من الهوية، والوصول المادي والمنطقي، والتشفير) تؤثر على سرية المعلومات. وذكر تقرير Government Accountability Office (2016b) أن نقاط الضعف التي تواجه سرية المعلومات لا تزال تشكل تحديا للمنظمات. غير أن دراسة Kannan et al. (2007) أكدت أن اختراق السرية لها تأثير سلبي منخفض على عائدات الشركات.

وفيما يتعلق بأثر مخاطر السلامة في أمن نظم المعلومات، فقد توصلت دراسة Mary (2011)، ودراسة Carstens، McCauley-Bell، Malone وDeMara (2004) إلى أن مخاطر السلامة (الأخطاء البشرية) تؤثر سلبا في أمن المعلومات والناتجة عن ضعف التدريب، أو الإهمال، أو عدم الوعي، أو ضغوط العمل. وذكر تقرير Lévy-Bencheton وDarra (2015) أن حذف البيانات المتعمد من قبل المستخدمين المخولين أو غير المخولين وأخطاء البرمجيات الفنية تؤثر سلبا في سلامة المعلومات. وتوقع تقرير McAfee Enterprise (2015) تعرض القطاع المالي لهجمات تستهدف سلامة البيانات. وقد أكد صحة هذه التوقعات تقرير Kaspersky (2017)، حيث شهد العالم عددا كبيرا من هجمات الفدية الخبيثة التي أثرت على سلامة المعلومات، وتسبب الهجوم في تعليق العمل في وزارة الداخلية الروسية، والاتصالات الأسبانية، والخدمات الصحية البريطانية.

وفيما يتعلق بأثر مخاطر التوافر في أمن نظم المعلومات، فقد توصلت دراسة Whitman (2004) إلى أن مزودي خدمات الاتصالات والطاقة الأكثر تأثرا بتوافر الخدمة وأنظمة المعلومات. وقد وثقت

https://doi.org/10.20428/JSS.27.1.5

تقارير الخدمات الأمنية Europol's European Cybercrime Centre (2015) مئات الهجمات يوميا، وذكر التقرير أن ما يقارب النصف من الدول الأعضاء في الاتحاد الأوربي تعتبر هجمات الحرمان من الخدمة الموزع التهديد الأكبر. وأشار تقرير Lévy-Bencheton وDarra (2015) إلى أن الحوادث البيئية والكوارث الطبيعية وانقطاع الطاقة تؤثر على عنصر التوافر. وكما وجدت دراسة Gordon et al. (2011) أن الاختراقات الأمنية المتعلقة بالتوافر لها تأثير سلبي كبير على عائدات الشركات.

مشكلة الدراسة:

تعاني منظمات الأعمال في اليمن من العديد من المخاطر التي تستهدف أمن نظم المعلومات، وتستغل هذه المخاطر الثغرات الأمنية في النظام، أو الشبكة، أو إجراءات أمن النظام، أو تنفيذ الضوابط. وقد جاء في تقرير الرقم القياسي العالمي للأمن السيبراني مجموعة من المؤشرات المستخدمة في قياس القدرات الوطنية في مجال الأمن في عام 2015م، حيث كان ترتيب اليمن (27) ورقمها القياسي (0.059)، وتعتبر درجة متدنية جدا (International Telecommunication Union (ITU), 2015). وفي عام 2017م جاءت اليمن في مجال الأمن السيبراني في الترتيب قبل الأخير (164) ورقمها القياسي (0.007) (ITU, 2017). وفي عام 2018م وصل ترتيب اليمن عالميا في مجال الأمن السيبراني إلى (172) من أصل (175) ورقمها القياسي (0.019) (ITU, 2019, 68). وأيضا أعطت أكاديمية الحوكمة الإلكترونية اليمن درجة متدنية في مجال الأمن الإلكتروني، حيث كان ترتيبها (148) من أصل (161)، وكان مؤشر الأمن السيبراني (7.79) (National Cyber Security Index, 2020). وقد أشار التقرير الصادر عن المؤسسة العامة اليمنية للاتصالات إلى أن إجمالي خسائر قطاع الاتصالات تقدر بـ(37) مليار ريال من مارس 2015م وحتى فبراير 2016م والناجم عن الحروب التي أدت إلى فقدان إيرادات مختلفة وتكاليف الصيانة والإصلاح. وأيضا ذكر التقرير أن من أهم الصعوبات التي تواجه شركات الاتصالات هو اعتمادها على المولدات والبطاريات على مدى (24) ساعة، نظرا للانعدام الكلي للطاقة العمومية ما ينذر بتوقف الخدمات (المركز الوطني للمعلومات، 2016).

وتناولت الصحافة في 30 إبريل 2014م حدوث خلل فني مما أدى إلى توقف خدمة الاتصالات لساعات، وتسبب ذلك في فقدان إيرادات واستياء المشتركين (الوحدوي نت، 2014). ورصد الخبراء في شركة Kaspersky تنصت وكالة الأمن القومي (NSA) على الحواسيب في (30) دولة ومنها اليمن، وقد استهدفت برامج التجسس الإلكترونية قطاع الاتصالات (Reuters, 2015).

وتناولت بعض الدراسات مخاطر أمن نظم المعلومات في الشركات العاملة في اليمن، حيث أشارت دراسة الربيدي (2010) إلى وجود مخاطر تكنولوجية متوسطة في العمليات المصرفية الإلكترونية في اليمن. ومنها الوصول غير المصرح به، وعدم سلامة تجهيز البيانات، وعدم القدرة على حماية خصوصية العملاء. وأيضا خلصت دراسة فاضل (2018) إلى وجود مخاطر تهدد أمن نظم المعلومات وبدرجات متفاوتة في البنوك التجارية العاملة في اليمن، وأن المخاطر تؤثر سلبا في أمن نظم المعلومات. وأشارت نتائج الدراسة الاستطلاعية التي قام بها الباحثان إلى وجود مخاطر تهدد أمن نظم المعلومات في شركات الاتصالات العاملة في اليمن. وقد أكد وزير الاتصالات في المؤتمر الأول لأمن المعلومات بصنعاء يونيو 2014م، أن اليمن لا يملك تشريعا يحفظ للناس خصوصياتهم ويحمي ممتلكاتهم. وقد تم تكليف مجموعة من المختصين لعمل مشروع قانون يقدم للحكومة لمناقشته وإقراره – ولم يصدر هذا القانون حتى اليوم –. ومن جانب آخر، أشار مدير المؤسسة العامة للاتصالات إلى أن المؤسسة تبنت مشروع مركز أمن المعلومات للاتصالات اليمنية الذي يعتبر نواة لمركز أمن المعلومات الوطني – حتى الآن لم يتم إنشاء هذا المركز – (المؤسسة العامة للاتصالات، 2014)، وبالتالي: تسعى الدراسة الحالية إلى الإسهام في قياس أثر مخاطر تكنولوجيا المعلومات (مخاطر السرية، ومخاطر السلامة، ومخاطر التوافر، والمخاطر العامة) في أمن نظم المعلومات لدى شركات الاتصالات العاملة في اليمن.

https://doi.org/10.20428/JSS.27.1.5

أسئلة الدراسة:

بناء على مشكلة الدراسة يمكن صياغة السؤال الآتي:

- **السؤال الرئيس: ما درجة تأثير مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات لدى شركات الاتصالات العاملة في اليمن؟ وسيتم الإجابة عن السؤال الرئيس من خلال الإجابة عن الأسئلة الفرعية الآتية:**
- **السؤال الفرعي الأول: ما درجة تأثير المخاطر المتعلقة بالسرية في أمن نظم المعلومات لدى شركات الاتصالات العاملة في اليمن؟**
- **السؤال الفرعي الثاني: ما درجة تأثير المخاطر المتعلقة بالسلامة في أمن نظم المعلومات لدى شركات الاتصالات العاملة في اليمن؟**
- **السؤال الفرعي الثالث: ما درجة تأثير المخاطر المتعلقة بالتوافر في أمن نظم المعلومات لدى شركات الاتصالات العاملة في اليمن؟**
- **السؤال الفرعي الرابع: ما درجة تأثير المخاطر العامة في أمن نظم المعلومات لدى شركات الاتصالات العاملة في اليمن؟**

أهداف الدراسة:

بناء على أسئلة الدراسة تم صياغة الأهداف الآتية:

الهدف الرئيس: قياس أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات لدى شركات الاتصالات العاملة في اليمن. ويتفرع الهدف الرئيس إلى مجموعة من الأهداف الفرعية الآتية:

- **الهدف الفرعي الأول: قياس أثر المخاطر المتعلقة بالسرية في أمن نظم المعلومات لدى شركات الاتصالات العاملة في اليمن.**
- **الهدف الفرعي الثاني: قياس أثر المخاطر المتعلقة بالسلامة في أمن نظم المعلومات لدى شركات الاتصالات العاملة في اليمن.**
- **الهدف الفرعي الثالث: قياس أثر المخاطر المتعلقة بالتوافر في أمن نظم المعلومات لدى شركات الاتصالات العاملة في اليمن.**
- **الهدف الفرعي الرابع: قياس أثر المخاطر العامة في أمن نظم المعلومات لدى شركات الاتصالات العاملة في اليمن.**

أهمية الدراسة:

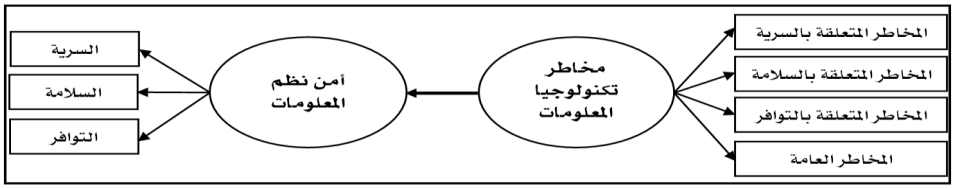
تتمثل أهمية هذه الدراسة في الآتي:

1) **قدمت أداة لقياس أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات لدى شركات الاتصالات مجتمع الدراسة، وذلك من خلال تطوير وتعديل أداة القياس التي قد تفيد الباحثين والمهتمين.**
2) **إضافة بُعد جديد (المخاطر العامة) إلى المتغير المستقل لأهمية دراسته لا سيما في قطاع الاتصالات، وتصنيف مخاطر تكنولوجيا المعلومات من حيث تأثيرها في أمن نظم المعلومات.**
3) **تسهم الدراسة في تعزيز أمن نظم المعلومات لدى شركات الاتصالات مجتمع الدراسة والحفاظ على سرية المعلومات وسلامتها وتوافرها من مخاطر تكنولوجيا المعلومات.**
4) **إمكانية استفادة مجلس الإدارة والإدارة التنفيذية في شركات الاتصالات داخل اليمن وخارجها، وذلك من خلال تقديم مجموعة من التوصيات للعمل بها خاصة فيما يتعلق بإنشاء إدارة لأمن المعلومات تعمل على بناء وتطبيق نظام لإدارة أمن المعلومات وفق معايير دولية، وكذلك إمكانية استفادة إدارة تكنولوجيا المعلومات وإدارة التدقيق الفني في تقييم أمن نظم المعلومات ودرجة المخاطر.**

https://doi.org/10.20428/JSS.27.1.5

النموذج المعرفي:

بناء على الخلفية النظرية والأدب السابق، يُمكننا بناء النموذج المعرفي للدراسة الحالية كما هو موضح في الشكل الآتي:



شكل (1): النموذج المعرفي للدراسة

فرضيات الدراسة:

- **الفرضية الرئيسية: يوجد أثر سلبي ذو دلالة إحصائية لمخاطر تكنولوجيا المعلومات في أمن نظم المعلومات لدى شركات الاتصالات العاملة في اليمن. ويتفرع من هذه الفرضية أربع فرضيات فرعية تتمثل بالآتي:**
- **الفرضية الفرعية الأولى: يوجد أثر سلبي ذو دلالة إحصائية لمخاطر السرية في أمن نظم المعلومات.**
- **الفرضية الفرعية الثانية: يوجد أثر سلبي ذو دلالة إحصائية لمخاطر السلامة في أمن نظم المعلومات.**
- **الفرضية الفرعية الثالثة: يوجد أثر سلبي ذو دلالة إحصائية لمخاطر التوافر في أمن نظم المعلومات.**
- **الفرضية الفرعية الرابعة: يوجد أثر سلبي ذو دلالة إحصائية للمخاطر العامة في أمن نظم المعلومات.**

منهج الدراسة:

اعتمدت الدراسة الحالية على المنهج التحليلي، وتم استخدام أساليب الإحصاء الاستدلالي في قياس أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات بالاعتماد على نمذجة المعادلة البنائية لقياس أثر تلك العلاقة.

مجتمع الدراسة وعينتها:

استهدفت الدراسة الحالية جميع شركات الاتصالات العاملة في اليمن وفقا لأسلوب الحصر الشامل، وعددها سبع شركات (تيليمن، المؤسسة العامة للاتصالات، يمن نت، إم تي إن، سبأفون، يمن موبايل، واي). ويتكون مجتمع الدراسة المستهدف من 356 مشاركا في إدارة تكنولوجيا المعلومات، وإدارة التدقيق الفني، وإدارة الرقابة والتحكم، وإدارة تشغيل الشبكة والإنترنت المتواجدة في المراكز الرئيسية لشركات الاتصالات في العاصمة صنعاء. وتم جمع المعلومات عن مجتمع الدراسة من خلال النزول الميداني، والرجوع إلى المختصين في إدارة الموارد البشرية، والمواقع الإلكترونية الخاصة بشركات الاتصالات، وكتاب الإحصاء السنوي الصادر عن الجهاز المركزي للإحصاء. وقد تم اختيار هذا القطاع كمجتمع للدراسة الحالية؛ نظرا لأهمية أمن المعلومات وحساسيتها في قطاع الاتصالات بشكل خاص واعتمادها على تكنولوجيا المعلومات بشكل كبير.

وقد تم توزيع الاستبانة على جميع عناصر المجتمع، وهي: 356 استبانة من خلال النزول الميداني المباشر والمتابعة المستمرة من قبل الباحثين، والاستعانة بموظفي الموارد البشرية، ومتعاونين، وتم استرداد 226 استبانة بنسبة 63 %، أما الاستبانات التي لم تسترد فعددها 130 استبانة بنسبة 37 %، والصالحة للتحليل 218 استبانة بنسبة 61 % من الاستبانات الموزعة. ويوضح الجدول الآتي عدد الاستبانات الموزعة والمستردة والصالحة للتحليل.

https://doi.org/10.20428/JSS.27.1.5

جدول (1): عدد الاستبانات الموزعة والمستردة والصالحة للتحليل

م	الشركات	المجتمع	الاستبانات الموزعة	الاستبانات المستردة	الاستبانات الصالحة للتحليل	الاستبانات الصالحة للتحليل بحسب الإدارات					الإجمالي
						نوع الاستجابة	تكنولوجيا المعلومات	التدقيق الفني	الرقابة والتحكم	تشغيل الشبكة والإنترنت	
1	شركة A	92	92	81	79	تقليدي	28	3	6	35	79
			% 100	% 88	% 86	إلكتروني	0	0	1	6	
2	شركة B	50	50	25	24	تقليدي	9	4	1	10	24
			% 100	% 50	% 48	إلكتروني	0	0	0	0	
3	شركة C	66	66	54	52	تقليدي	24	5	4	19	52
			% 100	% 82	% 79	إلكتروني	0	0	0	0	
4	شركة D	30	30	22	22	تقليدي	0	0	0	0	22
			% 100	% 73	% 73	إلكتروني	12	2	2	6	
5	شركة E	52	52	16	16	تقليدي	0	0	0	7	16
			% 100	% 31	% 31	إلكتروني	5	0	0	4	
6	شركة F	45	45	20	17	تقليدي	8	0	4	5	17
			% 100	% 44	% 38	إلكتروني	0	0	0	0	
7	شركة G	21	21	8	8	تقليدي	0	0	0	0	8
			% 100	% 38	% 38	إلكتروني	4	0	0	4	
	الإجمالي	356	356	226	218	الإجمالي	90	14	18	96	218
	النسبة	% 100	% 100	% 63	% 61	النسبة	% 41.3	% 6.4	% 8.3	% 44	% 100

ملاحظة: تم ترميز شركات الاتصالات مجتمع الدراسة بناء على طلب بعض المستجيبين.

وحدة التحليل:

وحدة التحليل في الدراسة الحالية تتمثل في المنظمة (شركات الاتصالات العاملة في اليمن)؛ كون أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات يقاس على مستوى المنظمة.

أداة الدراسة:

اعتمدت الدراسة الحالية في تطوير الاستبانة على الجانب النظري، والدراسات السابقة، وقد تم بناء أمن نظم المعلومات (المتغير التابع) بالاعتماد على دراسة Chang وWang (2011)، Seno et al. (2015) الذي يتكون من ثلاثة أبعاد: (1) السرية: وقد تم قياسها من خلال 9 فقرات، (2) السلامة: وقد تم قياسها من خلال 9 فقرات، (3) التوافر: وقد تم قياسها من خلال 10 فقرات.

وتم بناء قائمة مخاطر تكنولوجيا المعلومات (المتغير المستقل) بالاعتماد على دراسة Carr Loch، وWarkenting (1992)، ودراسة Riad (2009)، ودراسة Schuessler (2009)، ودراسة Whitman (2004)، والذي يتكون من أربعة أبعاد: (1) مخاطر السرية: تم قياسها من خلال 8 فقرات، (2) مخاطر السلامة: تم قياسها من خلال 6 فقرات، (3) مخاطر التوافر: تم قياسها من خلال 6 فقرات، (4) المخاطر العامة: تم قياسها من خلال 8 فقرات.

وقد تم تقسيم الاستبانة إلى محورين رئيسين، المحور الأول: يتعلق بجمع بيانات عن واقع أمن نظم المعلومات في شركات الاتصالات (المتغير التابع). والمحور الثاني: يتعلق بجمع بيانات عن درجة المخاطر التي تتعرض لها أنظمة المعلومات في شركات الاتصالات (المتغير المستقل). ويُبين الجدولين (2، 3) أبعاد وفقرات المتغيرين.

https://doi.org/10.20428/JSS.27.1.5

جدول (2): أبعاد وفقرات أمن نظم المعلومات

المتغير التابع	الأبعاد	عدد الفقرات	م	الفقرات تقيس الفقرات الآتية واقع أمن نظم المعلومات في شركة الاتصالات التي تعمل بها.
أمن نظم المعلومات	السرية	9	1	المعلومات الحساسة في الشركة محمية من الكشف.
			2	خصوصية المعلومات الشخصية للعملاء محمية من الكشف.
			3	المعلومات المنقولة عبر الشبكة محمية من الاعتراض.
			4	حسابات المستخدمين على المواقع الإلكترونية الخاصة بالشركة محمية من الكشف.
			5	يتم الوصول إلى المعلومات من قبل موظفي الشركة بحسب صلاحيتهم.
			6	تفرض الشركة رقابة صارمة على الوصول المادي إلى السيرفرات ووسائط التخزين.
			7	معلومات الشركة محمية من الوصول غير المصرح به.
			8	إعدادات نظام الشركة محمية من الوصول غير المصرح به.
			9	يتم مشاركة معلومات الشركة بين الأطراف المصرح لها.
	السلامة	9	10	محتوى معلومات الشركة المخزنة دقيقة.
			11	محتوى معلومات الشركة المنقولة مطابقة للمعلومات الأصلية.
			12	معلومات الشركة محمية ضد التعديل غير المصرح به.
			13	إعدادات نظام الشركة محمية ضد التعديل غير المصرح به.
			14	يوفر نظام الشركة إمكانية التعرف على أي تعديلات حدثت للمعلومات.
			15	نظام الشركة يحمي المستخدمين من هجمات انتحال الهوية.
			16	يوفر نظام الشركة إمكانية التعرف على أي إتلاف حدث للمعلومات.
			17	معلومات الشركة محمية من الإتلاف غير المصرح به.
			18	أجهزة النظام ووسائط التخزين بالشركة محمية من الإتلاف.
	التوافر	10	19	تطبيقات نظم معلومات الشركة متاحة للمستخدمين المخولين.
			20	الموقع الخاص بالشركة متاح للمستخدمين دون انقطاع.
			21	الخدمات التي تقدمها أنظمة الشركة متاحة للمستخدمين طوال الوقت دون أي انقطاع.
			22	سيرفرات الشركة متاحة للمستخدمين المخولين باستمرار.
			23	النظام يُمكن المخولين من الوصول إلى المعلومات عند الطلب.
			24	توفر الشركة طاقة احتياطية للاستخدام عند انقطاع التيار.
			25	توفر الشركة موقع بديل لتشغيل نظم المعلومات في حال حدوث كوارث.
			26	سرعة الاستجابة لحوادث الأمن واستئناف العمليات.
			27	إمكانية استرداد بيانات وأنظمة الشركة بسرعة.
			28	نظام الشركة قادر على تلبية احتياجات جميع المستخدمين.

وقد تم استخدام مقياس ليكرت السباعي للمتغير التابع وفقا لدراسة Chang وWang (2011)، وKankanhalli، Teo، Tan وWei (2003). حيث تشير (7) إلى موافق بشدة، وهي تعني أن أمن نظم المعلومات في شركات الاتصالات مرتفع جدا، ويشير (1) إلى غير موافق بشدة، وهي تعني أن أمن نظم المعلومات في شركات الاتصالات منخفض جدا.

https://doi.org/10.20428/JSS.27.1.5

جدول (3): أبعاد وفقرات مخاطر تكنولوجيا المعلومات

المتغير المستقل	الأبعاد	عدد الفقرات	م	الفقرات تتعرض أنظمة المعلومات في شركة الاتصالات التي تعمل بها للمخاطر الآتية:
مخاطر تكنولوجيا المعلومات	المخاطر المتعلقة بالسرية	8	29	هجمات التنصت (اعتراض شبكة الاتصالات أو التقاط البيانات أثناء نقلها داخل وخارج الشركة).
			30	هجمات كسر كلمة المرور (الوصول إلى كلمة المرور المخزنة في النظام أو المنقولة عبر الشبكة).
			31	الوصول غير المصرح به لنظام الشركة من قبل أطراف خارجية مثل المهاجمين.
			32	الوصول غير المصرح به لنظام الشركة من قبل أطراف داخلية مثل الموظفين.
			33	الأفعال المتعمدة المتعلقة بالسرقة (معدات أو معلومات الشركة).
			34	الأفعال المتعمدة المتعلقة بالابتزاز (الابتزاز بالكشف عن المعلومات).
			35	هجمات الاصطياد الإلكتروني، انتحال هوية أشخاص أو منظمة يثق بهم الضحية باستخدام وسائل تقنية.
			36	هجمات الهندسة الاجتماعية (القدرة على التمثيل واقناع الضحية بالإفصاح عن المعلومات السرية).
	المخاطر المتعلقة بالسلامة	6	37	الإدخال غير المتعمد للبيانات الخاطئة من قبل الموظفين.
			38	إتلاف البيانات غير المتعمد من قبل الموظفين.
			39	الإدخال المتعمد للبيانات الخاطئة من قبل الموظفين.
			40	إتلاف البيانات المتعمد من قبل الموظفين.
			41	أخطاء البرمجيات الفنية مثل الأخطاء التي يقع فيها المبرمجين أثناء كتابة البرامج.
			42	التقادم التكنولوجي مثل الأجهزة والأنظمة المتقادمة.
	المخاطر المتعلقة بالتوافر	6	43	هجمات الحرمان من الخدمة (منع المستخدمين الشرعيين من الوصول إلى الخدمة).
			44	تفجير البريد الإلكتروني (إغراق بريد الشركة بالرسائل مما يؤدي إلى توقفه عن العمل).
			45	الكوارث الطبيعية مثل الحرائق، والصواعق، والعواصف.
			46	الكوارث السياسية مثل الحروب، وانقطاع الطاقة الكهربائية.
			47	أعطال أجهزة النظام الفنية.
			48	أعطال معدات الشبكة الفنية.
	المخاطر العامة	8	49	قرصنة الهاتف (إجراء مكالمات مجانية، أو الوصول غير المشروع إلى المعلومات، أو تعطيل الخدمة)
			50	هجمات الانتحال مثل انتحال عنوان IP، أو البريد الإلكتروني، أو موقع الويب، أو هوية المتصل.
			51	فيروسات الحاسوب (تستنسخ نفسها عندما يتناقل المستخدمين الملف المصاب).
			52	ديدان الحاسوب (قادرة على استنساخ نفسها تلقائيا).
			53	أحصنة طروادة (برنامج يخفي طبيعته الحقيقية ويكشف عن سلوكه المُعد عند تفعيله).
			54	برامج التجسس الإلكتروني (برامج خفية تراقب استخدام الحاسوب وجمع المعلومات عن المستخدم وإرسالها للمهاجم).
			55	القنبلة المعلوماتية (برنامج معين يظل ساكن حتى تاريخ محدد أو ظهور حدث معين ثم يبدأ بتدمير المعلومات).
			56	هجمات الرسائل المزعجة أو غير المرغوب فيها مثل رسائل الهاتف القصيرة، أو البريد الإلكتروني، أو مواقع التواصل.

https://doi.org/10.20428/JSS.27.1.5

وتم استخدام مقياس ليكرت السباعي للمتغير المستقل وفقا لدراسة Davis (1997)، Loch et al. (1992)، وSchuessler (2009). حيث تشير (7) إلى أعلى درجة، وهي تعني أن المخاطر في شركات الاتصالات مرتفعة جدا، ويشير (1) إلى أقل درجة، وهي تعني أن المخاطر التي تواجه أنظمة المعلومات في شركات الاتصالات منخفضة جدا.

اختبار صدق المحتوى للأداة:

تم عرض الاستبانة على عدد من المحكمين المتخصصين في الجوانب الأكاديمية والمهنية والإحصائية والبالغ عددهم 26، للتأكد من أن الاستبانة تتضمن فقرات كافية وشاملة لقياس درجة مخاطر تكنولوجيا المعلومات ومستوى أمن نظم المعلومات، وقد أبدى المحكمون آراءهم وقدموا مقترحاتهم وملحوظاتهم حول تعديل بعض الفقرات، أو إعادة صياغتها، أو حذفها، أو إضافة فقرات جديدة بحيث تزيد من تحسين الاستبانة، وبناء على ملحوظات المحكمين تم إجراء التعديلات اللازمة.

اختبار صدق وثبات أداة الدراسة: تم اختبار الصدق والثبات عن طريق تقييم نموذج القياس كما سيأتي.

الأساليب الإحصائية المستخدمة:

تم استخدام طريقة المربعات الصغرى الجزئية (SmartPLS) في تقييم نموذج القياس، وتقييم النموذج البنائي، وتقييم معاملات المسار واختبار الفرضيات.

عرض نتائج الدراسة ومناقشتها:

أولا: نتائج تقييم نموذج الدراسة:

تم تقييم نموذج الدراسة الحالية وتحليل بيانات الدراسة باستخدام حزمة برامج المربعات الصغرى الجزئية (SmartPLS) الإصدار (v.3.2.8) على مرحلتين، المرحلة الأولى: تقييم نموذج القياس. والمرحلة الثانية: تقييم النموذج البنائي.

تقييم نموذج القياس:

يشير نموذج القياس إلى العلاقات بين الأبعاد وفقراتها وكيفية قياس الأبعاد من خلال الفقرات، ويعتبر الصدق والثبات معيارين أساسيين يُستخدمان في تقييم نموذج القياس. حيث يتم تقييم الاتساق الداخلي للتحقق من ثبات أداة القياس، وتقييم صدق التقارب والتمايز للتحقق من دقة أداة القياس (Sekaran & Bougie, 2016).

تقييم نموذج القياس الانعكاسي لأبعاد الدرجة الأولى:

نموذج القياس الانعكاسي نوع من أنواع نماذج القياس، حيث تكون العلاقة السببية من الأبعاد إلى الفقرات ويكون السهم المؤشر من البُعد إلى الفقرة، ويجب أن يكون الارتباط بين الفقرات عاليا داخل البُعد، ويمكن حذف بعض الفقرات دون أن تؤثر على البُعد كليا (Hair et al., 2019; Hair et al., 2017).

وقد تم تقييم نموذج القياس الانعكاسي من خلال استخدام المقاييس الإحصائية كالتشبع الخارجي لتقييم ثبات المؤشر، واستخدام الثبات المركب وألفا كرونباخ لتقييم ثبات الاتساق الداخلي للأبعاد، واستخدام متوسط التباين المفسر لتقييم صدق التقارب. واستخدام طريقة التشبعات المتقاطعة وطريقة نسبة أحادية وتغاير السمة لتقييم صدق التمايز (Hair et al., 2017).

الخطوة الأولى: تقييم ثبات المؤشر:

يتحقق الثبات عندما يكون التشبع الخارجي لكل مؤشر أعلى من (0.708)؛ وهذا يعني أن البُعد يفسر أكثر من 50% من تباين فقراته (Hair et al., 2019).

https://doi.org/10.20428/JSS.27.1.5

ويتضح من نتائج تقييم ثبات المؤشر أن عدد الفقرات التي يجب حذفها (9) فقرات، موضحة وفقا للأسباب الآتية: (1) تم حذف الفقرات التي تشبعها أقل من (0.708) وقد أدى حذفها إلى زيادة الثبات المركب ومتوسط التباين المفسر، وهي: مخاطر السلامة 42، ومخاطر التوافر 46، والمخاطر العامة 51. (2) تم حذف الفقرات التي تقل من صدق التمايز بين الأبعاد على الرغم من أن تشبعها أعلى من (0.708) وفقا لـ Hair et al. (2017)، وهي: السرية 1، والسلامة 10، والسلامة 11، والسلامة 13، والتوافر 19، والتوافر 22.

وبعد حذف تلك الفقرات التي يؤدي حذفها إلى زيادة الثبات المركب أو متوسط التباين المفسر أو تقلل من صدق التمايز بين الأبعاد. يمكن القول: إن جميع الفقرات المتبقية تقيس الأبعاد بدرجة عالية من الثبات. ويلاحظ أن جميع الفقرات المتبقية تشبعها أعلى من (0.708). ويعرض الجدول الآتي التشبع الخارجي للفقرات المتبقية بعد الحذف.

جدول (4): تقييم نموذج القياس (ثبات المؤشر، والاتساق الداخلي، وصدق التقارب)

المتغيرات	الأبعاد	الفقرات	التشبع Loadings	ألفا كرونباخ (α)	الثبات المركب (CR)	متوسط التباين المفسر (AVE)
أمن نظم المعلومات	السرية	السرية 2	0.765	0.918	0.933	0.637
		السرية 3	0.827			
		السرية 4	0.771			
		السرية 5	0.755			
		السرية 6	0.815			
		السرية 7	0.860			
		السرية 8	0.844			
		السرية 9	0.738			
	السلامة	السلامة 12	0.782	0.906	0.928	0.682
		السلامة 14	0.820			
		السلامة 15	0.792			
		السلامة 16	0.867			
		السلامة 17	0.867			
		السلامة 18	0.822			
	التوافر	التوافر 20	0.813	0.932	0.943	0.676
		التوافر 21	0.835			
		التوافر 23	0.821			
		التوافر 24	0.806			
		التوافر 25	0.751			
		التوافر 26	0.865			
		التوافر 27	0.830			
		التوافر 28	0.853			

https://doi.org/10.20428/JSS.27.1.5

جدول (4): يتبع

المتغيرات	الأبعاد	الفقرات	التشبع Loadings	ألفا كرونباخ (α)	الثبات المركب (CR)	متوسط التباين المفسر (AVE)
مخاطر تكنولوجيا المعلومات	مخاطر السرية	مخاطر السرية 29	0.762	0.924	0.938	0.654
		مخاطر السرية 30	0.836			
		مخاطر السرية 31	0.858			
		مخاطر السرية 32	0.793			
		مخاطر السرية 33	0.785			
		مخاطر السرية 34	0.815			
		مخاطر السرية 35	0.794			
		مخاطر السرية 36	0.821			
	مخاطر السلامة	مخاطر السلامة 37	0.772	0.868	0.905	0.655
		مخاطر السلامة 38	0.811			
		مخاطر السلامة 39	0.858			
		مخاطر السلامة 40	0.848			
		مخاطر السلامة 41	0.754			
	مخاطر التوافر	مخاطر التوافر 43	0.758	0.831	0.880	0.596
		مخاطر التوافر 44	0.721			
		مخاطر التوافر 45	0.799			
		مخاطر التوافر 47	0.822			
		مخاطر التوافر 48	0.756			
	المخاطر العامة	المخاطر العامة 49	0.795	0.923	0.938	0.684
		المخاطر العامة 50	0.829			
		المخاطر العامة 52	0.785			
		المخاطر العامة 53	0.849			
		المخاطر العامة 54	0.899			
		المخاطر العامة 55	0.829			
		المخاطر العامة 56	0.798			

الخطوة الثانية: تقييم ثبات الاتساق الداخلي:

يُستخدم الثبات المركب أو الكلي Composite Reliability (CR) في تقييم ثبات الاتساق الداخلي للأبعاد، وتشير القيم العليا إلى مستويات أعلى من الثبات. وتتراوح قيم الثبات المقبولة بين (0.70–0.95)، وتعتبر قيم الثبات بين (0.60–0.70) مقبولة في البحث الاستكشافي. وقد يُستخدم ألفا كرونباخ Cronbach's alpha (α) كمقياس آخر في تقييم الثبات ويستخدم نفس قيم الثبات المركب ولكنه أقل دقة (Hair et al., 2019).

وقد أظهرت النتائج في الجدول (4) أن قيم الثبات المركب تراوحت بين (0.88) و (0.94)، وقيم ألفا كرونباخ تراوحت بين (0.83) و (0.93) لكل بُعد. وتشير هذه النتيجة إلى أن الاتساق الداخلي لجميع الأبعاد ذات ثبات عالٍ، وبالتالي يمكن القول إن جميع الأبعاد تقيس المتغيرين المستقل والتابع بدرجة عالية من الثبات.

الخطوة الثالثة: تقييم صدق التقارب:

يتم تقييم صدق التقارب من خلال استخدام متوسط التباين المفسر Average variance extracted (AVE) **لجميع الفقرات في كل بُعد. ويمكن تربيع تشبع كل فقرة في البُعد وحساب متوسط القيمة للوصول إلى متوسط التباين المفسر. والحد الأدنى المقبول لمتوسط التباين المفسر هو** (0.50) **أو أعلى ويشير هذا إلى أن البُعد يفسر** 50% **أو أكثر من التباين في الفقرات التي تكون البُعد** (Hair et al., 2019).

وقد تراوحت قيم متوسط التباين المفسر لجميع الأبعاد بين (0.59) **و** (0.68) **في الجدول** (4)**، ويتضح أن قيم متوسط التباين المفسر لكل بُعد تقع ضمن النطاق الموصى به، ويشير هذا إلى أن البُعد يفسر ما نسبته** (0.50) **أو أكثر من التباين في الفقرات التابعة له، وهذا يدل على تحقق صدق التقارب.**

الخطوة الرابعة: تقييم صدق التمايز:

يعني صدق التمايز أن البُعد يختلف عن الأبعاد الأخرى في النموذج (Hair et al., 2017)**، بعبارة أخرى، يجب أن يكون لكل بُعد ارتباط مع مؤشراته أكبر من ارتباطه مع مؤشرات الأبعاد الأخرى** (Hair et al., 2017)**. ويتم قياس صدق التمايز من خلال طريقة التشبعات المتقاطعة وطريقة نسبة أحادية وتغاير السمة.**

1) **طريقة التشبعات المتقاطعة:**

يتحقق صدق التمايز بين المؤشرات إذا كان التشبع الخارجي للمؤشر مع بُعده أعلى من تشبعاته المتقاطعة مع الأبعاد الأخرى (ارتباط الفقرة ببُعدها أعلى من ارتباطها مع بقية الأبعاد الأخرى) (Hair et al., 2017)**. وقد أظهرت نتائج تقييم التشبعات المتقاطعة في الجدول** (5) **أن تشبعات الفقرات التابعة (القيم الغامقة) لكل بُعد أعلى من تشبعاتها المتقاطعة مع الأبعاد الأخرى. وتشير هذا النتيجة إلى عدم تداخل فقرات القياس فيما بينها (أي تتميز فقرات كل بُعد عن فقرات الأبعاد الأخرى).**

جدول (5)**: تقييم صدق تمايز الفقرات باستخدام طريقة التشبعات المتقاطعة**

الفقرات / الأبعاد	التوافر	السرية	السلامة	المخاطر العامة	مخاطر التوافر	مخاطر السلامة	مخاطر السرية
التوافر 20	**0.813**	0.523	0.643	-0.237	-0.311	-0.268	-0.286
التوافر 21	**0.835**	0.609	0.657	-0.316	-0.345	-0.313	-0.297
التوافر 23	**0.821**	0.694	0.740	-0.306	-0.339	-0.258	-0.331
التوافر 24	**0.806**	0.551	0.571	-0.195	-0.229	-0.210	-0.213
التوافر 25	**0.751**	0.424	0.496	-0.270	-0.340	-0.225	-0.325
التوافر 26	**0.865**	0.595	0.643	-0.325	-0.379	-0.324	-0.380
التوافر 27	**0.830**	0.566	0.656	-0.319	-0.354	-0.340	-0.420
التوافر 28	**0.853**	0.589	0.664	-0.354	-0.418	-0.323	-0.413
السرية 2	0.523	**0.765**	0.573	-0.323	-0.347	-0.308	-0.333
السرية 3	0.564	**0.827**	0.643	-0.384	-0.327	-0.334	-0.419
السرية 4	0.471	**0.771**	0.613	-0.424	-0.354	-0.327	-0.397
السرية 5	0.479	**0.755**	0.563	-0.282	-0.233	-0.285	-0.261
السرية 6	0.545	**0.815**	0.614	-0.294	-0.284	-0.276	-0.271
السرية 7	0.640	**0.860**	0.691	-0.377	-0.325	-0.327	-0.339
السرية 8	0.630	**0.844**	0.673	-0.352	-0.308	-0.334	-0.322
السرية 9	0.558	**0.738**	0.539	-0.301	-0.335	-0.228	-0.279

https://doi.org/10.20428/JSS.27.1.5

جدول (5): يتبع

الفقرات / الأبعاد	التوافر	السرية	السلامة	المخاطر العامة	مخاطر التوافر	مخاطر السلامة	مخاطر السرية
السلامة 12	0.668	0.694	**0.782**	-0.293	-0.326	-0.284	-0.328
السلامة 14	0.615	0.509	**0.820**	-0.161	-0.257	-0.212	-0.298
السلامة 15	0.694	0.646	**0.792**	-0.405	-0.387	-0.357	-0.426
السلامة 16	0.588	0.588	**0.867**	-0.198	-0.244	-0.227	-0.358
السلامة 17	0.626	0.717	**0.867**	-0.386	-0.363	-0.383	-0.441
السلامة 18	0.615	0.654	**0.822**	-0.190	-0.264	-0.261	-0.327
المخاطر العامة 49	-0.339	-0.397	-0.350	**0.795**	0.565	0.548	0.628
المخاطر العامة 50	-0.324	-0.387	-0.306	**0.829**	0.672	0.596	0.700
المخاطر العامة 52	-0.273	-0.319	-0.236	**0.785**	0.565	0.531	0.548
المخاطر العامة 53	-0.302	-0.329	-0.253	**0.849**	0.600	0.546	0.577
المخاطر العامة 54	-0.297	-0.351	-0.288	**0.899**	0.670	0.618	0.648
المخاطر العامة 55	-0.236	-0.338	-0.269	**0.829**	0.584	0.556	0.620
المخاطر العامة 56	-0.296	-0.368	-0.251	**0.798**	0.628	0.531	0.568
مخاطر التوافر 43	-0.322	-0.345	-0.294	0.618	**0.758**	0.596	0.564
مخاطر التوافر 44	-0.354	-0.367	-0.332	0.567	**0.721**	0.569	0.543
مخاطر التوافر 45	-0.349	-0.334	-0.318	0.591	**0.799**	0.534	0.632
مخاطر التوافر 47	-0.316	-0.246	-0.275	0.586	**0.822**	0.545	0.556
مخاطر التوافر 48	-0.251	-0.189	-0.212	0.467	**0.756**	0.483	0.470
مخاطر السلامة 37	-0.294	-0.333	-0.317	0.522	0.521	**0.772**	0.520
مخاطر السلامة 38	-0.248	-0.277	-0.257	0.580	0.573	**0.811**	0.546
مخاطر السلامة 39	-0.314	-0.357	-0.298	0.544	0.580	**0.858**	0.590
مخاطر السلامة 40	-0.249	-0.287	-0.277	0.558	0.612	**0.848**	0.593
مخاطر السلامة 41	-0.299	-0.283	-0.283	0.549	0.600	**0.754**	0.542
مخاطر السرية 29	-0.306	-0.265	-0.304	0.496	0.542	0.443	**0.762**
مخاطر السرية 30	-0.357	-0.350	-0.387	0.573	0.596	0.528	**0.836**
مخاطر السرية 31	-0.340	-0.375	-0.420	0.625	0.617	0.619	**0.858**
مخاطر السرية 32	-0.302	-0.357	-0.375	0.627	0.559	0.570	**0.793**
مخاطر السرية 33	-0.308	-0.321	-0.313	0.597	0.578	0.534	**0.785**
مخاطر السرية 34	-0.361	-0.358	-0.360	0.583	0.542	0.573	**0.815**
مخاطر السرية 35	-0.376	-0.311	-0.364	0.638	0.620	0.564	**0.794**
مخاطر السرية 36	-0.325	-0.338	-0.344	0.665	0.636	0.624	**0.821**

2) **طريقة نسبة أحادية وتغاير السمة:**

يجب أن تكون قيمة نسبة أحادية وتغاير السمة Heterotrait-monotrait Ratio (HTMT) **أصغر من الـ** (1)، **وعندما يكون الارتباط أقرب إلى** (1) **فإنه يدل على عدم وجود صدق تمايزي، ويتحقق صدق التمايز إذا كان متوسط ارتباطات الفقرات في الأبعاد لا تتجاوز نسبة** (0.85) (Hair et al., 2019).

https://doi.org/10.20428/JSS.27.1.5

وقد أشـارت النتائج في الجدول (6) إلى أن جميع قيم نسبة أحادية وتغاير السمة (HTMT) تتراوح بين (0.35) كحد أدنى و(0.84) كحد أعلى، ويلاحظ أن هذه القيم أقل من (0.85)، حيث تشير هذه النتيجة إلى صـدق تمايز الأبعاد، وعدم وجود ارتباط عالٍ بين البُعـد وبقية الأبعاد الأخرى، وأن البُعد مختلف عن بقية الأبعاد الأخرى.

جدول (6): تقييم صدق التمايز باستخدام طريقة نسبة أحادية وتغاير السمة (HTMT)

الأبعاد	التوافر	السرية	السلامة	المخاطر العامة	مخاطر التوافر	مخاطر السلامة	مخاطر السرية
التوافر							
السرية	0.746						
السلامة	0.835	0.840					
المخاطر العامة	0.379	0.464	0.358				
مخاطر التوافر	0.462	0.438	0.420	0.835			
مخاطر السلامة	0.381	0.423	0.392	0.760	0.833		
مخاطر السرية	0.436	0.444	0.478	0.803	0.817	0.769	

تقييم نموذج القياس الانعكاسي لأبعاد الدرجة الثانية:

اقتـرح الباحثون العديـد من الطرق في تحديد وقيـاس الأبعاد من الدرجة الثانيـة في نمذجة المعادلة البنائيـة القائمة على المربعات الصغرى الجزئيـة (PLS-SEM)، وأبرزها ثلاث طرق، وهي: 1) الطريقة الهرميـة (Wold, 1982). 2) طريقـة المرحلتـين: والـتي تنقسـم إلى قسـمين المدمجـة والمنفصلـة (Agarwal & Karahanna, 2000, 678). 3) الطريقـة الهجينة (Wold, 1982). وقد اسـتخدمت الدراسـة الحالية طريقة المرحلتين؛ كونها الأنسب؛ لأن عدد الفقرات في الأبعاد غير متساوية، واعتمدت الدراسة في تقييم نموذج القياس الانعكاسي من الدرجة الثانية على طريقة المرحلتين المنفصلة، حيث يتم قياس أبعاد الدرجة الأولى في المرحلة الأولى بدون قياس أبعاد الدرجة الثانية، ومن ثم يتم اسـتخدام المتوسطات المعيارية لأبعاد الدرجة الأولى كمؤشرات لأبعاد الدرجة الثانية في المرحلة الثانية.

وقد أشارت نتائج تقييم النموذج القياسي الانعكاسي من الدرجة الثانية إلى الآتي:

1) ثبات المؤشر (الأبعاد من الدرجة الأولى):

يتضح من الجدول (7) أن تشبع جميع قيم مؤشرات المتغيرات أكبر من (0.708)، وهذا يشير إلى أن أبعاد الدرجة الأولى تتمتع بثبات عالٍ، حيث تظهر كمؤشرات لأبعاد الدرجة الثانية.

2) ثبات الاتساق الداخلي (الأبعاد من الدرجة الثانية):

يتضـح من الجدول (7) أن جميع قيم الثبات المركـب وقيم ألفا أعلى من (0.70) وأقل من (0.95)، وهذا يشير إلى أن الاتساق الداخلي لأبعاد الدرجة الثانية ذو ثبات عالٍ.

3) صدق التقارب (الأبعاد من الدرجة الثانية):

يظهر في الجدول (7) أن جميع قيم متوسط التباين المفسر أكبر من (0.50)؛ وهذا يدل على وجود تقارب بين كل بُعد من الدرجة الثانية وأبعاده من الدرجة الأولى.

https://doi.org/10.20428/JSS.27.1.5

جدول (7): تقييم ثبات المؤشر، والاتساق الداخلي، وصدق التقارب

الأبعاد من الدرجة الثانية (المتغيرات)	الأبعاد من الدرجة الأولى (المؤشرات)	التشبع Loadings	ألفا كرونباخ (α)	الثبات المركب (CR)	متوسط التباين المفسر (AVE)
أمن نظم المعلومات	السرية	0.901	0.899	0.937	0.832
	السلامة	0.927			
	التوافر	0.907			
مخاطر تكنولوجيا المعلومات	مخاطر السرية	0.897	0.909	0.936	0.785
	مخاطر السلامة	0.861			
	مخاطر التوافر	0.895			
	المخاطر العامة	0.891			

4) صدق التمايز (الأبعاد من الدرجة الثانية):

يلاحظ من الجدول (8) أن قيم نسبة أحادية وتغاير السمة (HTMT) أقل من (0.85)؛ وهذا يشير إلى صدق تمايز الأبعاد من الدرجة الثانية، وأنه لا يوجد ارتباط عالٍ بين البُعد من الدرجة الثانية وبقية الأبعاد الأخرى، وأن كل بُعد من الدرجة الثانية مختلف عن الأبعاد الأخرى.

جدول (8): تقييم صدق تمايز أبعاد الدرجة الثانية باستخدام طريقة (HTMT)

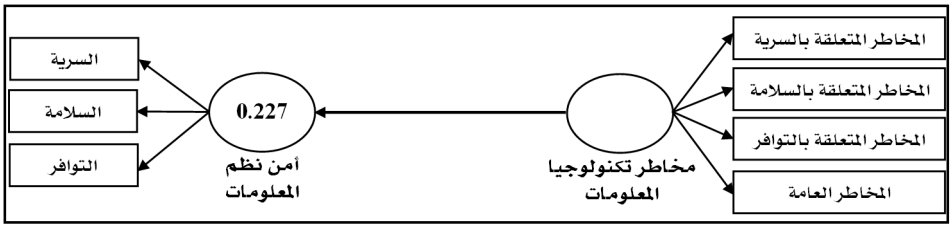
المتغيرات	مخاطر تكنولوجيا المعلومات	أمن نظم المعلومات
مخاطر تكنولوجيا المعلومات		
أمن نظم المعلومات	0.524	

تقييم النموذج البنائي للمتغيرات الكلية من الدرجة الثانية:

أكدت نتائج تقييم نموذج القياس الانعكاسي صدق وثبات أداة القياس، وفي هذه المرحلة سوف يتم تقييم النموذج البنائي باستخدام نمذجة المعادلة البنائية القائمة على المربعات الصغرى الجزئية (PLS-SEM).

أولا: معامل التحديد (R^2)

تختلف قيمة معامل التحديد (R^2) من (0) إلى (1)، حيث تعني (0) أن التباين المفسر منخفض، وتعني (1) أن التباين المفسر مرتفع. ويمكن تحديد قدرة النموذج على تفسير المتغير التابع من خلال قيمة (R^2) التي تقدر بـ (0.67) أو (0.33) أو (0.19) قوية، أو متوسطة، أو ضعيفة على التوالي وفقا لـ Chin (1998). بينما يرى Falk وMiller (1992) أن أقل قيمة مقبولة لمعامل التحديد (R^2) هي (0.10). ويوضح الشكل (2) نتائج تقييم معامل التحديد.



شكل (2): تقييم معامل التحديد

https://doi.org/10.20428/JSS.27.1.5

يتضح من الشكل (2) أن قيمة معامل التحديد لأمن نظم المعلومات (0.227)؛ وهذا يشير إلى أن مخاطر تكنولوجيا المعلومات تفسر ما نسبته 22.7 % من التباين في أمن نظم المعلومات، وبالتالي تمثل هذه القيمة مستوى متوسطا.

ثانيا: ملائمة التنبؤ (Q^2)

تعتمد هذه الطريقة على إجراء Blindfolding[1] لحساب وتفسير قيمة ملائمة التنبؤ (Q^2) من خلال المقارنة بين القيم المتوقعة والأصلية والاختلافات بينهما هي قيمة ملائمة التنبؤ (Q^2)، وعندما تكون الاختلافات بينهما صغيرة؛ فهذا يعني أن نموذج المسار يتمتع بدقة تنبؤية عالية. وعندما تكون قيمة ملائمة التنبؤ (Q^2) أكبر من الصفر فإنها تعني أن النموذج لديه دقة تنبؤ، أما إذا كانت مساوية للصفر أو أقل فإن هذا مؤشر إلى عدم دقة النموذج من حيث التنبؤ (Hair et al., 2019). وكقاعدة عامة، فإن قيم (Q^2) أعلى من (0) أو (0.15) أو (0.35) والتي تشير إلى أن الملائمة التنبوية صغيرة أو متوسطة أو كبيرة لنموذج مسار (PLS) على التوالي (Hair et al., 2019). والجدول (9) يُبين نتائج تقييم ملائمة النموذج للتنبؤ.

جدول (9): تقييم ملائمة التنبؤ (Q^2) على مستوى أبعاد المتغير التابع

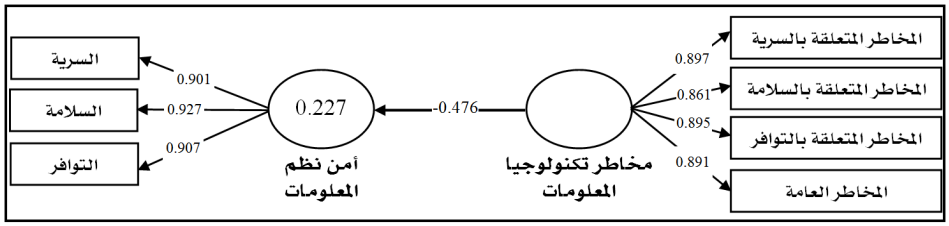
الأبعاد	(SSO) مجموع مربع المشاهدات	(SSE) مجموع مربع أخطاء التنبؤ	Q^2 (=1−SSE/SSO) ملائمة التنبؤ	التقدير
السرية	218	138.706	0.364	عالية
السلامة	218	140.526	0.355	عالية
التوافر	218	131.671	0.396	عالية

يظهر الجدول (9) نتائج تقييم ملائمة التنبؤ (Q^2) على مستوى أبعاد أمن نظم المعلومات، حيث كانت دقة وملائمة التنبؤ لأبعاد السرية والسلامة والتوافر عالية، وجميعها أكبر من (0.35).

تقييم معاملات المسار:

يتم تقييم معاملات المسار من خلال إجراء Bootstrapping[2] بغرض الحصول على تقديرات لعلاقات النموذج البنائي التي تمثل العلاقات المفترضة بين المتغيرات. وتقع قيم معاملات المسار ضمن نطاق (±1)، حيث تمثل القيم القريبة من (+1) علاقات إيجابية قوية، والقيم القريبة من (−1) علاقات سلبية قوية، وعادة ما تكون ذات دلالة إحصائية. وكلما كانت معاملات المسار المقدرة أقرب إلى (0) كانت العلاقات ضعيفة (Hair et al., 2017)، حيث إن التغيير في المتغير المستقل بوحدة واحدة ينشأ عنها تغيير في المتغير التابع بقدر حجم معامل المسار على فرض ثبات جميع المتغيرات الأخرى ومعاملات مساراتها.

وقد تم إجراء Bootstrapping باستخدام حزمة برامج المربعات الصغرى الجزئية (PLS) لاختبار الفرضيات المقترحة بين متغيرات الدراسة الحالية. ويوضح الشكل (3) نتائج تقييم معاملات المسار.



شكل (3): تقييم معاملات المسار

[1] Blindfolding هي تقنية إعادة استخدام العينة، تسمح بحساب قيمة Q^2 لـ Stone-Geisser (Geisser, 1974; Stone, 1974)، والتي تمثل معيار تقييم للملائمة التنبؤية التي تم التحقق منها عبر نموذج مسارPLS.

[2] Bootstrapping هي تقنية إعادة أخذ العينات المستخدمة لتقدير الإحصائيات الخاصة بالمجتمع عن طريق أخذ عينات من مجموعة البيانات مع الاستبدال.

https://doi.org/10.20428/JSS.27.1.5

نتائج اختبار فرضيات الدراسة:

أولا: اختبار الفرضية الرئيسية:

يوجد أثر سلبي ذو دلالة إحصائية لمخاطر تكنولوجيا المعلومات في أمن نظم المعلومات في شركات الاتصالات العاملة في اليمن. ويظهر الجدول (10) نتائج اختبار هذه الفرضية.

جدول (10): اختبار الفرضية الرئيسية

المسار	معامل المسار β	الانحراف المعياري	إحصائية t	مستوى الدلالة p
مخاطر تكنولوجيا المعلومات -> أمن نظم المعلومات	-0.476	0.071	6.691	0.000

تشير النتائج في الجدول (10) إلى أن مخاطر تكنولوجيا المعلومات تؤثر سلبا في أمن نظم المعلومات، حيث كانت قيمة معامل المسار (β=-0.476)، وقيمة (t=6.691) دالة إحصائيا عند مستوى دلالة أقل من (0.01). وهذا يعني أن التغيير (الزيادة) في مخاطر تكنولوجيا المعلومات بوحدة واحدة ينشأ عنها انخفاض في أمن نظم المعلومات بنسبة 47.6 %، وبالتالي تدعم هذه النتيجة الفرضية الرئيسية.

وهذه النتيجة التي تم التوصل إليها تتفق مع نظرية أمن المعلومات (Horne, Ahmad, & Maynard, 2016) التي تشير إلى أن العلاقة بين المخاطر والمعلومات سلبية، حيث تؤدي المخاطر إلى انتهاك سرية المعلومات وسلامتها وتوافرها بشكل سلبي. وتتفق هذه النتيجة أيضا مع دراسة Gordon et al. (2011) التي توصلت إلى أن اختراقات أمن المعلومات بشكل عام لها تأثير سلبي دال إحصائيا على قيمة الشركات في سوق الأوراق المالية، وكذلك دراسة Cavusoglu et al. (2004) التي توصلت إلى أن الاختراقات الأمنية كفئة عامة لها تأثير سلبي ذو دلالة إحصائية على الشركات. وأيضا وجدت دراسة Ishiguro et al. (2006) أن الاختراقات الأمنية كفئة عامة لها تأثير سلبي قوي ذو دلالة إحصائية على قيمة الشركات في سوق الأوراق المالية. ووجدت دراسة Riad (2009) أن المخاطر تؤثر سلبا في أمن المعلومات. وبالمقابل تختلف هذه النتيجة مع دراسة Kannan et al. (2007) التي أشارت إلى أن اختراقات أمن المعلومات كفئة عامة لها تأثير سلبي ولكن غير دال إحصائيا على عائدات الشركات في سوق الأوراق المالية التي تعاني من الاختراقات.

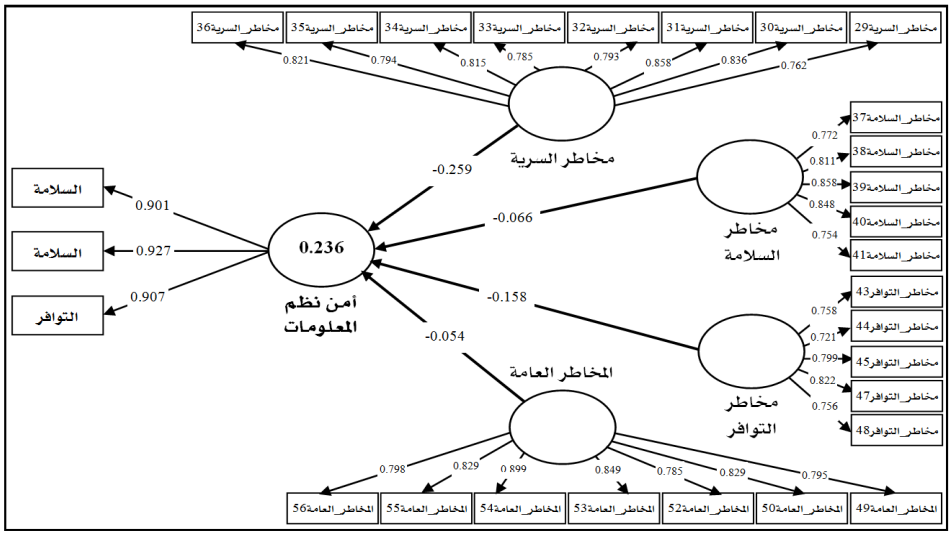
وتؤكد نتيجة الدراسة الحالية واتفاقها إلى حد كبير مع الدراسات السابقة تعرض أنظمة المعلومات في الشركات لمخاطر متعددة ومتنوعة. وقد يرجع ذلك إلى ضعف، أو استغلال المهاجمين ثغرات في أنظمة الحماية، أو استخدام أساليب الهندسة الاجتماعية والتي تستهدف المعلومات السرية، أو سلامتها، أو توافرها، وتؤثر هذه الهجمات بشكل سلبي في أنظمة المعلومات، وتؤدي إلى إلحاق أضرار بالشركات. وفي الواقع، نجد أن بعض الشركات استطاعت صد مثل هذه الهجمات، وشركات أخرى تمكّن المهاجمين من اختراق أنظمتها، وقد أثرت تلك الهجمات عليها وأصابها الضرر.

ثانيا: اختبار الفرضيات الفرعية للفرضية الرئيسية:

ويتفرع من الفرضية الرئيسية أربع فرضيات فرعية، تتمثل بالآتي:

1) **يوجد أثر سلبي ذو دلالة إحصائية للمخاطر المتعلقة بالسرية في أمن نظم المعلومات.**
2) **يوجد أثر سلبي ذو دلالة إحصائية للمخاطر المتعلقة بالسلامة في أمن نظم المعلومات.**
3) **يوجد أثر سلبي ذو دلالة إحصائية للمخاطر المتعلقة بالتوافر في أمن نظم المعلومات.**
4) **يوجد أثر سلبي ذو دلالة إحصائية للمخاطر العامة في أمن نظم المعلومات.**

ويوضح الشكل (4) نتائج تقييم معاملات المسار لكل بُعد من أبعاد المتغير المستقل مع المتغير التابع.



شكل (4): تقييم معاملات المسار لكل بُعد من أبعاد المتغير المستقل مع المتغير التابع

يوضح الشكل (4) قيمة معامل المسار على الخط الواصل بين أبعاد مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات، وأيضا يظهر في الشكل قيمة معامل التحديد (R^2) لأمن نظم المعلومات بمقدار (0.236)، وهذا يشير إلى أن أبعاد مخاطر تكنولوجيا المعلومات (مخاطر السرية، ومخاطر السلامة، ومخاطر التوافر، والمخاطر العامة) تُفسر ما نسبته 23.6 % من التباين في أمن نظم المعلومات. ويبين الجدول (11) نتائج اختبار الفرضيات الفرعية للفرضية الرئيسية.

جدول (11): اختبار الفرضيات الفرعية للفرضية الرئيسية

م	المسار	معامل المسار β	الانحراف المعياري	إحصائية t	مستوى الدلالة p
1	مخاطر السرية -> أمن نظم المعلومات	-0.259	0.117	2.222	0.013
2	مخاطر السلامة -> أمن نظم المعلومات	-0.066	0.094	0.701	0.242
3	مخاطر التوافر -> أمن نظم المعلومات	-0.158	0.086	1.829	0.034
4	المخاطر العامة -> أمن نظم المعلومات	-0.054	0.106	0.513	0.304

فيما يتعلق بالفرضية الفرعية الأولى: يتضح من الجدول (11) أن مخاطر السرية تؤثر سلبا في أمن نظم المعلومات في شركات الاتصالات، حيث كانت قيمة معامل المسار (β=-0.259)، وقيمة (t=2.222) دالة إحصائيا عند مستوى دلالة أقل من (0.05)، هذا يعني أنه كلما زادت مخاطر السرية بوحدة واحدة انخفض أمن نظم المعلومات بنسبة (25.9 %)، وتدعم هذه النتيجة الفرضية الفرعية الأولى للفرضية الرئيسية.

وتتفق هذه النتيجة مع دراسة Gordon et al. (2011) التي أشارت إلى أن الاختراقات الأمنية المتعلقة بالسرية لها تأثير سلبي على عائدات الشركات. أيضا، وجد الباحثون Campbell et al. (2003) أن الاختراقات الأمنية المتعلقة بالوصول غير المصرح به للمعلومات السرية لها تأثير سلبي دال إحصائيا على القيمة السوقية للشركة. وأكدت دراسة Ishiguro et al. (2006) أن اختراق المعلومات السرية لها تأثير سلبي كبير دال إحصائيا على عائدات الشركات في سوق الأوراق المالية. وقد أشار الباحثون Norman، Hamid، Hanifa وTamrin (2017) إلى أن الاصطياد الإلكتروني، والهندسة الاجتماعية، وهجمات الالتقاط تؤثر سلبا في سرية المعلومات. وأشارت دراسة Azees et al. (2016) إلى أن هجوم التنصت، والالتقاط، وسرقة الهوية تؤثر سلبا في سرية المعلومات.

https://doi.org/10.20428/JSS.27.1.5

وهـذه النتيجة تدل علـى أن أنظمة المعلومات تعاني أكثر من المخاطر التي تسـتهدف السـرية (هجمات التنصت، والوصـول غير المصرح به، والأفعال المتعمدة، والاصطياد الإلكتروني، والهندسـة الاجتماعية) والناتجة عن اسـتغلال نقـاط الضعف لأنظمة المعلومـات، ويؤكد ذلك تقريـر Trend Micro (2015) الـذي يشـير إلى أن 60 % مـن نقـاط الضعـف تؤثر على سـرية المعلومـات. وأيضا أكـد تقرير مكتب المسـاءلة الحكوميـة (Government Accountability Office, 2016b) أن نقـاط الضعـف لا تزال تشـكل تحديا يواجه سـرية المعلومات. كما نجد أن مخاطر السـرية قد تـؤدي إلى إلحاق أضرار بشـركات الاتصالات وعملائها، مثل فقدان الميزة التنافسية وفقدان الثقة والإضرار بالسمعة. حيث ذكر Donaldson et al. (2015) أن الاختراقات المتعلقة بالسرية تتصدر عناوين الصحف اليومية كالوصول إلى معلومات عن الحسـابات المصرفية، وأرقام بطاقات الائتمان، وأسرار الشركة. وذكرت دراسة Ernst و Young (2015) أحداث وقعت كسرقة ملايين الحسابات المصرفية وتسريب كم هائل من المعلومات السرية والتي أدت إلى إلحاق أضرار بالمنظمات وعملائها.

وفيمـا يتعلق بالفرضيـة الفرعية الثانية: تشـير النتائج في الجدول (11) إلى أن مخاطر السـلامة لها تأثير سـلبي في أمن نظم المعلومات غير دال إحصائيا، حيث كانت قيمة معامل المسار (β=-0.066)، وقيمة (t=0.701) غـير دالة إحصائيا عند مسـتوى دلالة أقل من (0.05). وهـذه النتيجة لا تدعم الفرضية الفرعية الثانية للفرضية الرئيسية.

وتختلـف هذه النتيجة مع ما ورد في تقريـر Lévy-Bencheton وDarra (2015) الذي ذكر أن حذف البيانات بشـكل متعمد من قبل المسـتخدمين المخولين أو غير المخولين وأخطاء البرمجيات الفنية تؤثر في سـلامة المعلومات. وكذلك أشـارت دراسـة Carstens et al. (2004)، وMary (2011) إلى أن مخاطر السـلامة (الأخطاء البشـرية) تؤثر سـلبا في أمن المعلومات والناتجة عن ضعف التدريب، أو الإهمال، أو عدم الوعي، أو ضغوط العمل. وأيضا توصلت دراسة Azees et al. (2016) إلى أن التعديل الخطأ يؤثر سـلبا في سـلامة البيانات. وكما توقع تقريـر McAfee (2015) المختص بأمـن المعلومات تعرض القطاع المالي لهجمات تستهدف سـلامة البيانات (فواتير المبيعات، وسجلات الهوية، وبطاقات التأمين، والحسابات المصرفية، وسيتبعها قطاعات أخرى)، ومن المحتمل سرقة ملايين الدولارات من خلال تعديل بيانات محددة في كـم كبير من المعاملات. ووفقـا لتقرير Kaspersky (2017) المختص بأمن المعلومات، نجد أن الأحداث الأمنية التي وقعت في 2017/4/14م تؤيد توقعات McAfee، حيث شـهد العالم عددا كبيرا من هجمات الفدية الخبيثة، وبعد ساعات قليلة من الهجوم تم رصد (45,000) هجوم في 74 دولة.

ونلاحـظ أن الدراسـات والتقارير في مجال الأمن والحوادث الأمنية التي وقعت تؤيد فرضية الدراسـة، ولكنهـا تختلف مع نتيجة الدراسـة الحالية، وقد يرجع سـبب الاختـلاف إلى الآتي: 1) نظرا لاختلاف أهمية أهداف الأمن (السرية والسلامة والتوافر) من قطاع إلى آخر، فمن المحتمل انخفاض أهمية سلامة المعلومـات في قطاع الاتصالات. 2) نظرا لاعتماد قطـاع الاتصالات على الإدخال الآلي بدلا من الإدخال اليـدوي فمن المتوقع انخفاض مخاطر السـلامة. 3) يلاحظ أن أغلب فقـرات هذا البُعد تتعلق بالإدخال والإتلاف المتعمد وغير المتعمد من قبل الموظفين، ومن المتوقع تحيز الموظفين عينة الدراسة في الاستجابة. وباعتقادي أن السبب الأخير هو الأقرب إلى الدقة.

وفيمـا يتعلق بالفرضية الفرعية الثالثة: أظهرت النتائج في الجـدول (11) أن مخاطر التوافر لها تأثير سـلبي في أمن نظـم المعلومات. ويتضـح أن قيمة معامل المسـار (β=-0.158)، وقيمـة (t=1.829) دالة إحصائيـا عند مسـتوى دلالة أقل من (0.05)؛ وهذا يعني أنه كلمـا زادت مخاطر التوافر بوحدة واحدة انخفض مسـتوى أمن نظم المعلومات بنسـبة (15.8 %). وتدعم هذه النتيجة الفرضية الفرعية الثالثة للفرضية الرئيسية.

https://doi.org/10.20428/JSS.27.1.5

وهـذه النتيجة تتفق مع دراسـة Whitman (2004) التي أشـارت إلى أن مـزودي خدمات الاتصالات والطاقـة الأكثـر تأثرا بتوافر الخدمـة وأمن المعلومات. أيضـا، تقارير الخدمـات الأمنية Europol's European Cybercrime Centre (2015)، الـتي وثقـت مئـات الهجمات يوميـا تؤكد أن ما يقارب النصـف مـن الدول الأعضـاء في الاتحاد الأوربي تعتبر هجمـات الحرمان من الخدمـة الموزع (DDoS) التهديد الأكبر. وكشفت أبحاث شركة Kaspersky (2016) المختص بأمن المعلومات تعرض مواقع Web في (70) دولـة لهجمـات الحرمان مـن الخدمة المـوزع (DDoS) في الربع الثاني من عـام 2016م. وكان تركيز مجرمي الإنترنت على المؤسسـات المالية. وأشارت دراسـة Lévy-Bencheton وDarra (2015) إلى أن الحـوادث البيئية والكوارث الطبيعية وانقطاع الطاقة تؤثر على عنصر التوافر. ووجدت دراسـة Gordon et al. (2011) أن الاختراقـات الأمنيـة المتعلقة بالتوافر لها تأثير سـلبي كبير على عائدات الشركات. وأيضا تعزز هذه النتيجة دراسة Anthony، Choi وGrabski (2006) التي توصلت إلى أن هناك علاقة سلبية قوية بين انقطاع الخدمة في مواقع Web (شكل من أشكال اختراق التوافر) والقيمة السوقية للشـركات، وأن الاختراقات تؤثر على عوائد الشركة، وبالمقابل اختلفت هذه النتيجة مع دراسة Hovav وD'arcy (2003) التي أشارت إلى أن الاختراقات الأمنية المتعلقة بهجمات الحرمان من الخدمة ليس لها تأثير على الشركات في سوق الأوراق المالية.

ويُفسـر تعـرض أنظمة المعلومات لمخاطر التوافـر (الحرمان من الخدمة، الكوارث الطبيعية والسياسـية، أعطال الأجهزة الفنية) في شـركات الاتصالات بدرجة أساسـية إلى مشـاكل الطاقة الكهربائية والتي تتمثل في غياب الطاقة العمومية تماما والاعتماد على المولدات والبطاريات، وكذلك الحروب التي تمر بها البلاد فقد تأثر قطاع الاتصالات بشـكل كبير مثل تعرض محطات وأبراج الاتصالات والكابلات الضوئية ومنشـآت القطـاع للتدمير وفقا للتقرير الصادر عن المؤسسـة العامة اليمنية للاتصـالات (المركز الوطني للمعلومـات، 2016)، وتؤدي هذه المخاطر إلى انقطاع الخدمـات وفقدان إيرادات وتتراوح الأضرار ما بين حجب الأنظمة مؤقتا إلى إتلاف الأنظمة بشكل كامل.

وفيمـا يتعلـق بالفرضية الفرعية الرابعة: أشـارت النتائج في الجـدول (11) إلى أن المخاطر العامة لها تأثير سـلبي غير دال إحصائيا في أمن نظم المعلومات، حيث كانت قيمة معامل المسار (β=-0.054)، وقيمة (t=0.513) غـير دالة إحصائيا عند مسـتوى دلالة أقل من (0.05)، وهـذه النتيجة لا تدعم الفرضية الفرعية الرابعة للفرضية الرئيسية.

وتتفق هذه النتيجة إلى حد ما مع دراسة Issac وVenkatachalam (2018) التي تشير إلى أن هجمات البرامج الضـارة منخفضة مقارنة بهجمات الحرمان من الخدمة والاصطياد الإلكتروني، وبالمقابل تختلف نتيجة هذه الدراسـة مع دراسـة Gordon et al. (2011) التي توصلت إلى أن غالبية اختراقات أمن المعلومات ناتجة عن الفيروسـات والتي تتسـبب في فقدان توافر المعلومات وسلامتها. وكذلك، ذكرت دراسة Norman et al. (2017) أن البرمجيات الضارة، وهجمات الانتحال، والرسـائل المزعجة تؤثر سـلبا في أمن المعلومات. وأشارت دراسة Azees et al. (2016) إلى أن هجمات البرامج الضارة والبريد المزعج يؤثر سلبا في سرية وسلامة وتوافر المعلومات.

ويُفسـر اتفاق واختلاف نتيجة الدراسة الحالية مع الدراسات السابقة فيما يتعلق بالمؤشرات إلى اختلاف البيئة التي أجريت فيها الدراسـة؛ كون الدراسات الأخرى أُجريت في بيئات مختلفة. أو اختلاف القطاع؛ كون الدراسـات أجريـت في قطاعات مختلفـة، أو أن مخاطر (قرصنة الهاتـف، والانتحال، والبرمجيات الضارة، والرسـائل المزعجة) منخفضة في قطاع الاتصالات؛ نظرا لفاعلية إجراءات الحماية واسـتخدام الضوابط الأمنية ذات العلاقة على نطاق واسع، أو أن الخدمات الإلكترونية التي يقدمها قطاع الاتصالات في اليمن محدودة، وبالتالي انخفاض هذه المخاطر. وقد تؤدي المخاطر العامة إلى توقف نظام المعلومات، وتوقف العمليات، وانخفاض الإنتاجية، وجميعها تسـبب خسـائر مالية. ويلاحظ أن الدراسات السابقة تناولت مؤشرات البُعد ولم تتناول بُعد المخاطر العامة.

https://doi.org/10.20428/JSS.27.1.5

الاستنتاجات:

بناء على نتائج اختبار الفرضيات ومناقشتها فقد خلصت الدراسة الحالية إلى العديد من الاستنتاجات، وهي:

1) **مصدر التأثير السلبي في أمن نظم المعلومات ناجم عن مخاطر السرية، يليها مخاطر التوافر؛ أي أن توسع عمليات الاتصال وازدياد الترابط بين أنظمة شركات الاتصالات والمشتركين (العملاء) وتحقق نمو في إجراء المعاملات عبر الإنترنت أدى ذلك إلى زيادة المخاطر المتعلقة بالسرية والتوافر، وتأثيرها في شركات الاتصالات العاملة في اليمن.**
2) **يتضح أن مصدر التأثير السلبي في سرية المعلومات بشركات الاتصالات يعود إلى المؤشرات المرتبطة بمخاطر السرية والمتمثلة في هجمات التنصت، وكسر كلمة المرور، والوصول غير المصرح به، والأفعال المتعمدة، والاصطياد الإلكتروني، والهندسة الاجتماعية.**
3) **نستنتج أن مصدر التأثير السلبي في توافر المعلومات بشركات الاتصالات يعود إلى المؤشرات المرتبطة بمخاطر التوافر والمتمثلة في الكوارث الطبيعية والسياسية، وأعطال الأجهزة الفنية، وهجمات الحرمان من الخدمة.**
4) **يتبين أن إجراءات الحماية في شركات الاتصالات العاملة في اليمن فاعلة ضد مخاطر السلامة والمخاطر العامة التي تواجه أمن نظم المعلومات.**

التوصيات:

بناء على الاستنتاجات التي تم التوصل إليها توصي الدراسة الحالية شركات الاتصالات العاملة في اليمن بالآتي:

1) **التأكيد على أهمية مواكبة أمن المعلومات للتطورات المتسارعة في تكنولوجيا المعلومات والاتصالات، ومراجعة جهود الردع والوقاية والكشف، ومعالجة جوانب القصور والثغرات الأمنية التي تؤدي إلى رفع مستوى أمن نظم المعلومات (السرية والتوافر) في شركات الاتصالات العاملة في اليمن، وخفض الأثر السلبي لمخاطر تكنولوجيا المعلومات.**
2) **مراجعة إجراءات حماية المعلومات ونظم المعلومات من الكشف والوصول غير المصرح به، وتقييد عمليات الوصول المصرح به، ونشر سياسة أمن المعلومات ورقابة تطبيقها؛ وذلك لخفض الأثر السلبي للمخاطر التي تستهدف سرية المعلومات في شركات الاتصالات.**
3) **مراجعة إجراءات حماية المعلومات ونظم المعلومات والخدمات من أعطال الأجهزة الفنية، والتقادم التكنولوجي، والكوارث السياسية، وهجمات الحرمان من الخدمة التي تستهدف عنصر التوافر في شركات الاتصالات.**
4) **تعزيز إجراءات الحماية من مخاطر التعديل أو الإتلاف غير المصرح به التي تستهدف سلامة المعلومات والأنظمة، وتعزيز إجراءات الحماية من الاستخدام غير المشروع لخدمات الاتصالات، وهجمات البرامج الضارة، وهجمات الخداع أو الانتحال. وإيلاء كل من السرية، والتوافر، والسلامة مزيدا من الاهتمام؛ كونهم الأكثر أهمية في قطاع الاتصالات.**
5) **دعم والتزام الإدارة العليا بأمن المعلومات، واعتماد موازنة أمنية كافية، وإنشاء إدارة خاصة بأمن المعلومات، وإنشاء مركز وطني لأمن المعلومات، وإعداد الجهات الرسمية قانون مكافحة الجرائم الإلكترونية وحماية البيانات الشخصية، وتوظيف الخبراء والمختصين في مجال أمن المعلومات. وهذه العوامل لها أثر إيجابي في رفع مستوى أمن المعلومات.**

https://doi.org/10.20428/JSS.27.1.5

المقترحات:

1) تم إجراء هذه الدراسة على قطاع الاتصالات فقط، وقد تكون النتائج غير قابلة للتعميم على بقية القطاعات؛ لذلك ينبغي توسيع نطاق البحث ليشمل أنواعا مختلفة من القطاعات، مثل إجراء دراسات مماثلة في البنوك، والمستشفيات، والجامعات.
2) إجراء مزيد من الأبحاث لاستكشاف العوامل التي تؤثر في أمن نظم المعلومات (السرية والسلامة والتوافر) سلبا وإيجابا، والتي قد تساعد في تعزيز أمن المعلومات.
3) تقترح الدراسة اختبار الدور المعدل لبرامج التوعية والتدريب بين الضوابط الأمنية وأمن نظم المعلومات.

المراجع:

الربيدي، محمد علي (2010)، حماية المعلومات المحاسبية في ظل مخاطر التكنولوجيا للعمليات المصرفية الإلكترونية: دراسة ميدانية في البنوك العاملة في اليمن، *مجلة كلية التجارة والاقتصاد*، *33*، 1-45.

زويلف، أنغام محسن حسن (2009)، طبيعة تهديدات أمن نظم المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على شركات التأمين الأردنية، *المجلة العربية للمحاسبة*، *12*(1)، 46-77.

الغثبر، خالد بن سليمان، والقحطاني، محمد بن عبدالله (2009)، *أمن المعلومات بلغة ميسرة* (ط1)، الرياض، السعودية: مكتبة الملك فهد الوطنية.

فاضل، عبدالكريم محمد يحيى (2018)، *تقييم مخاطر أمن نظم المعلومات المحاسبية المحوسبة لدى البنوك التجارية في اليمن: دراسة تطبيقية* (أطروحة دكتوراه غير منشورة)، جامعة دمشق، سوريا.

القحطاني، ذيب بن عايض (2015)، *أمن المعلومات* (ط1)، الرياض، السعودية: مكتبة الملك فهد الوطنية.

المركز الوطني للمعلومات (2016)، *أكثر من 37 مليار ريال خسائر مؤسسة الاتصالات منذ بدء الحرب: تقرير المؤسسة العامة للاتصالات*، استرجع من https://yemen-nic.info/news/detail.php?ID=72258

المؤسسة العامة للاتصالات (يونيو 26، 2014)، *بدء أعمال مؤتمر أمن المعلومات بصنعاء*، استرجع من https://bit.ly/3g1SXpp

الوحدوي نت (2014)، *خلل فني يوقف خدمة الاتصالات*، استرجع من https://bit.ly/3slEwi4

Agarwal, R., & Karahanna, E. (2000). Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS Quarterly, 24*(4), 665-694.

Ahmadzadegan, M. H., Elmusrati, M., & Mohammadi, H. (2013). Secure communication and VoIP threats in next generation networks. I*nternational Journal of Computer and Communication Engineering, 2*(5), 630-634.

AlKalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). Information Security compliance in organizations: an institutional perspective. *Data and Information Management, 1*(2), 104-114.

American Institute of Certified Public Accountants (AICPA). (2015). *25th anniversary edition of the North America top technology initiatives survey results*. Durham, North Carolina: AICPA.

https://doi.org/10.20428/JSS.27.1.5

Anthony, J. H., Choi, W., & Grabski, S. (2006). Market reaction to e-commerce impairments evidenced by website outages. *International Journal of Accounting Information Systems, 7*(2), 60-78.

Arsenie-Samoil, M. D. (2011). Security of the accounting information system infrastructure. *Ovidius University Annals, Economic Sciences Series, 11*(1), 1339-1345.

Azees, M., Vijayakumar, P., & Deborah, L. J. (2016). Comprehensive survey on security services in vehicular ad-hoc networks. I*ET Intelligent Transport Systems, 10*(6), 379-388.

Bafghi, A. A. S. T. (2014). Status and security of accounting information systems in Iranian organizations. *International Journal of Economy, Management and Social Sciences, 3*(12), 71-76.

Brown, C. V., DeHayes, D. W., Hoffer, J. A., Martin, E. W., & Perkins, W. C. (2012). *Managing information technology* (7th ed.). Hoboken, New Jersey: Prentice Hall.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431-448.

Carstens, D. S., McCauley-Bell, P. R., Malone, L. C., & DeMara, R. F. (2004). Evaluation of the human impact of password authentication practices on information security. *Informing Science Journal, 7*, 67-85.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce, 9*(1), 70-104.

Chang, K. C., & Wang, C. P. (2011). Information systems resources and information security. *Information Systems Frontiers, 13*(4), 579-593.

Cherdantseva, Y., & Hilton, J. (2015). Understanding information assurance and security. *Journal of Organizational and End User Computing, 16*(3), 1-48.

Chin, W. W. (1998). Issues and opinion on structural equation modeling. *MIS Quarterly, 22*(1), 7-16.

Cisco. (2015). *Annual security report*. San Jose, CA, USA: Cisco Systems, Inc.

Committee on National Security Systems (2015). *Committee on National Security Systems (CNSS) glossary*. Ft Meade, Maryland: CNSS Secretariat (IE414), National Security Agency.

Davis, C. E. (1997). An assessment of accounting information security. *The CPA Journal, 67*(3), 28-34.

Deloitte. (2006). *Protecting the digital assets: The 2006 technology, media and telecommunications security survey*. London, United Kingdom: Deloitte Touche Tohmatsu Limited (DTTL).

Deloitte. (2014). *Global cyber executive briefing: Lessons from the front lines*. London, United Kingdom: Deloitte Touche Tohmatsu Limited (DTTL).

Deloitte. (2016). *Cyber opportunity analysis report 2016: Positioned to lead*. London, United Kingdom: Deloitte Touche Tohmatsu Limited (DTTL).

Department for Culture Media and Sport (DCMS). (2016). *Cyber security breaches survey: Main report*. London: Department for Culture Media and Sport.

Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2015). *Enterprise cybersecurity: How to build a successful cyberdefense program against advanced threats*. New York: Apress.

Ernst & Young. (2012). *Fighting to close the gap: EY's 15th annual global information security survey (GISS)*, Bahamas, The Caribbean: EYGM Limited.

Ernst & Young. (2015). *Creating trust in the digital world: EY's 18th annual global information security survey (GISS)*, Bahamas, The Caribbean: EYGM Limited.

Europol's European Cybercrime Centre (EC3). (2015). *The internet organised crime threat assessment (IOCTA)*. The Hague, Netherlands: Europol's European Cybercrime Centre.

Falk, R. F., & Miller, N. B. (1992). *A primer for soft modeling* (1st ed.). Akron, Ohio: University of Akron Press.

Feruza, Y. S., & Kim, T. H. (2007). IT security review: Privacy, protection, access control, assurance and system security. *International Journal of Multimedia and Ubiquitous Engineering, 2*(2), 17-32.

Geisser, S. (1974). A predictive approach to the random effect model. *Biometrika, 61*(1), 101-107.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs?. *Journal of Computer Security, 19*(1), 33-56.

Government Accountability Office (Jun 29, 2016b). *Information security: FDIC implemented controls over financial systems, but further improvements are needed*. Retrieved from https://www.gao.gov/products/gao-16-605

Government Accountability Office (May 18, 2016a). *Information security: Agencies need to improve controls over selected high-impact systems.* Retrieved from https://www.gao.gov/products/gao-16-501

Hair, J. F., Hult, G. T., Ringle, C., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling* (2nd ed.). Newcastle upon Tyne, United Kingdom: Sage.

https://doi.org/10.20428/JSS.27.1.5

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review, 31*(1), 2-24.

Horne, C. A., Ahmad, A., & Maynard, S, B. (2016). *A theory on information security*. In the Proceedings of the 27th Australasian Conference on Information Systems (ACIS2016). University of Wollongong, Australia.

Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review, 6*(2), 97-121.

International Organization for Standardization (ISO) (2010). *Information technology – Security techniques – Information security management system implementation guidance* (1st ed.). Geneva, Switzerland: International Organization for Standardization.

International Organization for Standardization (ISO) (2010). *Information technology – Security techniques – Information security risk management* (2nd ed.). Geneva, Switzerland: International Organization for Standardization.

International Organization for Standardization (ISO) (2014). *ISO/IEC 27000:2014: Information technology – Security techniques – Information security management systems – Overview and vocabulary* (3rd ed.). Canada: Praxiom Research Group Limited.

International Organization for Standardization (ISO) (2018). *ISO/IEC 27000:2014: Information technology – Security techniques – Information security management systems – Overview and vocabulary* (5th ed.). Geneva, Switzerland: International Organization for Standardization.

International Telecommunication Union (ITU) (2015). *Global cybersecurity index and cyberwellness profiles*. Switzerland, Geneva: Telecommunication Development Sector and ABI research.

International Telecommunication Union (ITU) (2017). *Global cybersecurity index (GCI)*. Switzerland Geneva: Telecommunication Development Sector and ABI research.

International Telecommunication Union (ITU). (2019). *Global cybersecurity index (GCI)*. Switzerland Geneva: Telecommunication Development Sector and ABI research.

Ishiguro, M., Tanaka, H., Matsuura, K., & Murase, I. (2006). *The effect of information security incidents on corporate values in the Japanese stock market*. In the International Workshop on the Economics of Securing the Information Infrastructure (WESII), 31 August – 1 September, Arlington, VA.

Issac, P. E., & Venkatachalam, S. (2018). Security threats faced by the Indian banks. *International Journal of Pure and Applied Mathematics, 119*(15), 1667-1679.

Joint Task Force Transformation Initiative. (2001). *Computer security underlying technical models for information technology security*. National Institute of Standards and Technology (NIST) special publication 800-33. Gaithersburg, Maryland: NIST.

Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments*. National Institute of Standards and Technology (NIST) special publication 800-30 revision 1. Gaithersburg, Maryland: NIST.

Joint Task Force Transformation Initiative. (2013). *Security and privacy controls for federal information systems and organizations*. National Institute of Standards and Technology (NIST) special publication 800-35 revision 4. Gaithersburg, Maryland: NIST.

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science, 32*, 489-496.

Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154.

Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce, 12*(1), 69-91.

Kaspersky (2016). *Threat intelligence report for the telecommunications industry*. Moscow, Russia: Kaspersky.

Kaspersky (2017). *KSN report: Ransomware in 2016-2017*. Moscow, Russia: Kaspersky.

Kissel, R. (ed.). (2013). *Glossary of key information security terms*. NISTIR 7298 revision 2. Gaithersburg, Maryland: NIST.

Lévy-Bencheton, C., & Darra, E. (2015). *Cyber security for smart cities: An architecture model for public transport*. Heraklion, Greece: The European Union Agency for Network and Information Security, Tech. Rep.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. *Mis Quarterly, 16*(2), 173-186.

Mary, M. (2011). *Towards minimizing human factors in end-user information security* (Master thesis). University of Zimbabwe, Harare, Zimbabwe.

McAfee Enterprise (Nov 09, 2015). *McAfee labs 2016 threats predictions report.* Retrieved from https://bit.ly/32rlCvK

National Cyber Security Index (2020). *148. Yemen*. Retrieved from https://ncsi.ega.ee/country/ye/467/#details

https://doi.org/10.20428/JSS.27.1.5

Norman, A. A., Hamid, S., Hanifa, M. M., & Tamrin, S. I. (2017). *Security threats and techniques in social networking sites: A systematic literature review.* In the Future Technologies Conference, 29–30 November, Vancouver, Canada.

Paulsen, C., & Toth, P. (2016). *Small business information security: The fundamentals*. NISTIR 7621 revision 1. Gaithersburg, Maryland: NIST.

Pricewaterhouse (PwC). (2014). *Information security breaches survey: technical report*. London: PwC.

Reuters (2015). *Millions of computers may be compromised by US spyware: Report*. United Kingdom: Telegraph Media Group Limited.

Rhodes-Ousley, M. (2013). *Information security: The complete reference*. United States: McGraw-Hill Education.

Riad, N. I. (2009). *Security of accounting information systems: A cross-sector study of UK companies*. (Doctoral dissertation), Cardiff University, Cardiff, Wales.

Richardson, R. (2010). *15th annual 2010 / 2011 computer crime and security survey.* San Francisco, California: Computer Security Institute (CSI)

Schuessler, J. H. (2009). *General deterrence theory: Assessing information systems security effectiveness in large versus small businesses* (Doctoral dissertation). University of North Texas, Denton, Texas.

Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach* (7th ed.). Hoboken, New Jersey: John Wiley & Sons.

Seno, S. A. H., Bidmeshk, O. G., & Ghaffari, K. (2015). *Information security diagnosis in electronic banking (case study: Tejarat bank's branches of Isfahan)*. In the 9th International Conference on e-Commerce in Developing Countries: With Focus on e-Business (ECDC), 16 April, Isfahan, Iran.

Stone, M. (1974). Cross-validatory choice and assessment of statistical predictions. *Journal of the Royal Statistical Society: Series B (Methodological), 36*(2), 111-133.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

Trend Micro (2015). *Report on cybersecurity and critical infrastructure in the Americas*. Irving, Texas: Trend Micro Incorporated.

Wallis, A. (June 13, 2018). *What is information security? Why it's important, job outlook and more*. Retrieved from https://bit.ly/3egU6H7

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management, 24*(1), 43-57.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security* (4th ed.). Boston, Massachusetts: Cengage Learning.

Wold, H. (1982). Soft modeling: the basic design and some extensions. In: K. G. Jöreskog & H. Wold (Eds.), *Systems under indirect observation: Causality, structure, prediction* (pp. 1-54). Amsterdam: North-Holland.

Arabic References:

Alghathbaru, Khalid bin Sulayman, Walqahtani, Muhamad bin Abdullah (2009), *'Amn almaelumat bilughat maysara* (t1), Alriyad, Alsaeudiati: Maktabat Almalik Fahd Alwataniat.

Almarkaz Alwataniu Lilmaelumat (2016). *'Akthar min 37 milyar rial khasayir muasasat alaitisalat mundh bad' alharb: Taqrir Almuasasat Alamat Lilaitisalat,* Ostarjae min https://yemen-nic.info/news/detail.php?ID=72258

Almuasasat Alamat Lilaitisalat (Yuniu 26, 2014). *Bid' 'aamal Mutamar 'Amn Almaelumat bi Sana'a,* Ostarjae min https://bit.ly/3g1SXpp

Alqahtani, Dhib bin 'Ayid (2015). *'Amn almaelumat* (t1), Alriyad, Alsaeudiatu: Maktabat Almalik Fahd Alwataniat.

Alrubidi, Muhamad Ali (2010). Himayat almaelumat almuhasbyt fi zili makhatir altiknulujia lileamaliaat almasrifiat al'iiliktruniati: Dirasat maydaniat fi Albunuik Alamilat fi Alyaman, *Majalat Kuliyat Altijarat Walaiqtisadi, 33*, 1-45.

Alwahdawi Net (2014). *Khalal faniy ywqf khidmat alaitisalat,* Ostarjae min https://bit.ly/3slEwi4

Fadil, Abdalkrim Muhamad Yahya (2018). *Taqyim makhatir 'amn nuzum almalumat almuhasabyt almuhawsabat lada albunuk altijariat fi Alyaman: Dirasat tatbiqia* (Otarawhat dukturah ghyr manshurata), Jamieatan Dimashqi, Suria.

Zuaylf, 'Angham Muhsin Hasan (2009). Tabieat tahdidat 'amn nazam almaelumat almhasbyt al'iiliktruniatu: Dirasat tatbiqiat alaa sharikat altaamin al'urduniyati, *Almajalat Alarabiat Lilmahasabati, 12*(1), 46-77.

https://doi.org/10.20428/JSS.27.1.5