

أثر مخاطر تكنولوجيا المعلومات في الضوابط الأمنية: دراسة ميدانية في شركات الاتصالات بصنعاء

الاستلام: 22/يونيو/2025م
التحكيم: 1/يوليو/2025م
القبول: 11/أكتوبر/2025م

نبيل حسان عبده الحميري^(*,1) Nabil Hassan Abdo Al-Hemyari^(1,*)

© 2026 University of Science and Technology, Sana'a, Yemen. This article can be distributed under the terms of the [Creative Commons Attribution \(CC BY\) license](#), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

© 2026 جامعة العلوم والتكنولوجيا، صنعاء، اليمن. يمكن إعادة استخدام المادة المنشورة حسب رخصة مؤسسة المشاع الإبداعي من فئة (CC BY) شريطة الاستشهاد بالمؤلف والمجلة.

¹ Assistant Professor of Accounting, University of Science and Technology, Sana'a, Yemen

¹ أستاذ المحاسبة المساعد، جامعة العلوم والتكنولوجيا، صنعاء، اليمن

عنوان المراسلة: nabelal2000@yahoo.com . n.hassan@ust.edu.ye

أثر مخاطر تكنولوجيا المعلومات في الضوابط الأمنية: دراسة ميدانية في شركات الاتصالات بصنعاء

الملخص:

هدفت الدراسة إلى قياس أثر مخاطر تكنولوجيا المعلومات في الضوابط الأمنية في شركات الاتصالات العاملة في صنعاء باتباع منهج تحليلي، ويتمثل مجتمع الدراسة في شركات الاتصالات بصنعاء، وقد تم استخدام أسلوب الحصر الشامل في جمع البيانات من 356 مشاركا باستخدام الاستبانة، وقد كان عدد الاستبانات الصالحة للتحليل 218 استبانة، وتم تحليل البيانات باستخدام نموذج المعادلة البنائية القائمة على المربعات الصغرى الجزئية (PLS-SEM)، وقد كشفت نتائج الدراسة أن مخاطر تكنولوجيا المعلومات تؤثر سلباً في الضوابط الأمنية، وأوصت الدراسة بضرورة تنفيذ المصادقة القوية متعددة العوامل، وإيلاء التحكم بالوصول قدراً كبيراً من الاهتمام، والتحقق من الثغرات في الضوابط الأمنية. **الكلمات المفتاحية:** الضوابط الأمنية، مخاطر تكنولوجيا المعلومات، شركات الاتصالات بصنعاء.

Impact of Information Technology Risks on Security Controls: A Field Study in Telecommunications Companies in Sana'a

Abstract:

This study aimed to assess the impact of information technology risks on security controls in telecommunications companies operating in Sana'a, following an analytical method. The study population consisted of telecommunications companies in Sana'a, and a comprehensive census method was used to collect data from 356 participants using a questionnaire. However, only 218 questionnaires were valid for analysis. Data were analyzed using partial least squares structural equation modeling (PLS-SEM). The study findings revealed that information technology risks have a negative impact on security controls. The study recommends the necessity of implementing strong multi-factor authentication, devoting especial attention to access control, and regularly identifying vulnerabilities in security controls.

Keywords: security controls, information technology risks, telecommunication companies in Sana'a.

المقدمة:

أتاح استخدام تكنولوجيا المعلومات والاتصالات (Information and Communication Technology [ICT]) في العمل المحاسبي إمكانيات وفرصاً كبيرة لخدمة المنظمة (زويلف، 2009)؛ حيث أسهم استخدامها في رفع القدرات التحليلية، وتحسين كفاءة المنظمة، وإنجاز العمليات بدقة وسرعة عالية، وإجراء المعاملات، وتقديم الخدمات عبر الإنترنت، وقد رافق استخدام تكنولوجيا المعلومات والاتصالات العديد من المخاطر (أي أن التطورات في الأجهزة والبرمجيات لم تكن خالية من المخاطر) التي تؤثر سلباً في أنظمة المعلومات المحاسبية (Daferighe & Udih, 2014; Jouini et al., 2014).

وهدف الإدارة الأساس هو حماية موارد المنظمة من الوصول غير المصرح به إلى الحواسيب والبرامج والمرافق، والحفاظ على سرية المعلومات، وسلامتها، وتوافرها من المخاطر التي تواجهها، ويتحقق هذا الهدف من خلال تصميم وتنفيذ الضوابط الأمنية بما في ذلك التحقق من الهوية أو المصادقة، والتحكم بالوصول (تقييد عمليات الوصول المصرح به، ومنع عمليات الوصول غير المصرح به)، والاستجابة للحوادث الأمنية، والتصدي لأنشطة الهجوم، وكشف الاختراقات، واستعادة النظام والعمليات والبيانات، وتعزيز الموقف الدفاعي (U.S. Government Accountability Office [GAO], 2016)، والغرض من هذه الضوابط الأمنية إما القضاء على الخطر، أو الحد من آثاره السلبية (Schuessler, 2013).

وقد تناولت دراسة Schuessler (2013)، ودراسة Riad (2009) الضوابط الأمنية المستخدمة في حماية بيانات وأنظمة الشركات من المخاطر كالتحكم بالوصول، والمصادقة، ومكافح البرامج الضارة، وتقنيات التشفير والجدران النارية، وسياسة الأمن، وتدقيق الأمن، والتخطيط للطوارئ، والتوعية والتدريب، وأشارت النتائج إلى وجود اتفاق نسبي، وهناك تباين واختلاف في استخدام الضوابط الأمنية، وفي مدى فاعليتها في منظمات الأعمال.

وقد أكد تقرير Lévy-Bencheton-Darra (2015) على أهمية التدابير اللازمة لمواجهة التنصت (Eavesdropping) أو التنصت على المكالمات الهاتفية (Wiretapping)، مثل استخدام الشبكات الخاصة الافتراضية، وتشفير البيانات، ونشر أنظمة كشف التسلل في الشبكة، وأهم تلك التدابير المنفذة: (1) التدابير المادية لمنع الوصول إلى المناطق المحظورة، مثل أجهزة الإنذار. (2) التدابير الرامية لحماية البيانات، مثل التشفير. (3) التدابير الرامية لمنع الوصول، مثل الجدران النارية. (4) الإجراءات المعتمدة على السياسة، مثل تنفيذ سياسة الأمن. (5) أدوات بعد وقوع الحادث، مثل سجل النشاط والنسخ الاحتياطي.

ومع ذلك، قد تنشأ ثغرات أمنية جديدة مع مرور الزمن ناتجة عن عوامل تنظيمية، وبيئية، وتكنولوجية تؤدي إلى ظهور مخاطر جديدة، وتصبح الضوابط الأمنية الحالية غير كافية (Joint Task Force Transformation Initiative [JTFTI], 2012)؛ حيث كشف تقرير JTFTI (2012) عن ثغرات أمنية في خطط الطوارئ، واستخدام تقنيات متقدمة، وقصور في تنفيذ المصادقة والتحكم بالوصول، وقصور في الجوانب التشريعية والتنظيمية. وقد أكدت دراسة Abu-Khadra & Hayale (2006) أن القطاع المصرفي الأردني يعاني من قصور في الوصول المادي والمنطقي، وأمن البيانات، والتعليق من الكوارث، وكشف تقرير GAO (2015) عن جوانب الضعف في الضوابط الأمنية التي شهادتها الوكالات الفدرالية المتمثل في ضعف التحكم بالوصول، وضعف إدارة إعداد البرامج والأجهزة، وضعف خطة استمرارية العمل، وأشارت دراسة Mbowe et al. (2014) إلى أن ثلثي المنظمات تقريباً لديها استراتيجيات غير كافية للضوابط، وأكثر من ثلثي المنظمات تعاني من ضعف في استخدام التوقيعات الرقمية، وتدقيق الأمن، وذكر تقرير Verizon (2025) أن 30% من الخروقات ناتجة عن استغلال الثغرات الأمنية، وفي تقرير Verizon (2023) اتضح أن 86% من عمليات الاختراق استغلت ثغرات في ضوابط التحقق من الهوية والتحكم بالوصول. وأكدت دراسة Nhan et al. (2025) أن الأنظمة التي لا تدار بدقة تسبب ثغرات أمنية خطيرة، مما يؤدي إلى مخاطر الاحتيال والأخطاء في التقارير المالية، وأن نقص معرفة الموظفين بأمن المعلومات يتسبب في حدوث ثغرات أمنية، مثل تنزيل برامج ضارة، أو استخدام كلمات مرور ضعيفة.

وقد تناولت بعض التقارير والدراسات المخاطر الأمنية؛ حيث أكد تقرير Deloitte (2013) أن شركات الاتصالات لا تزال تواجه مخاطر أمنية جديدة وبشكل مرتفع، وذكر تقرير Deloitte (2014) أن استهداف شركات الاتصالات زاد، مثل التنصت على خطوط الهاتف، والردشة عبر الإنترنت، والوصول إلى البيانات الشخصية، والوصول إلى خدمات مكلفة، مثل المكالمات الدولية، وتوصل تقرير Deloitte (2006) إلى أن ثلث الاختراقات التي عانت منها شركات الاتصالات أدت إلى حدوث خسائر مالية كبيرة، وإلحاق أضرار بالسمعة والعلامة التجارية، وتوقف النظام، وفقدان إيرادات، وأشار تقرير Deloitte (2014) إلى أن الهجمات التي استهدفت شركات الاتصالات أدت إلى إلحاق أضرار كبيرة بسرية المعلومات، وأثارت مخاوف العملاء المتعلقة بالخصوصية، وبالتالي فقدان الثقة، وأشار تقرير Australian Cyber Security Centre (2015) إلى أن 43% من المنظمات الأسترالية لم تفصح عن الحوادث الأمنية خوفاً من فقدان ثقة عملائها، وذكرت دراسة Lee (2025) أن 61% من شركات الاتصالات تعرضت للتهديدات المتقدمة المستمرة (Advanced Persistent Threats)، وظهور ثغرات في بروتوكول نظام الإشارة رقم 7 (SS7) Signaling System No. 7 (SS7) تمكن من اعتراض المكالمات، وتتبع الموقع واختطاف الرسائل النصية القصيرة، وزادت هجمات حجب الخدمة الموزع بنسبة 175% بين عامي 2020 و2022، ومتوسط تكلفة خرق البيانات \$4.72 مليون لكل حادثة، وتؤثر الثغرات الأمنية في ثقة العملاء؛ حيث إن 65% من العملاء فقدوا الثقة في مزودي الخدمة بعد اختراق بياناتهم، وأنهى 31% من العملاء علاقتهم بالشركة، وذكر تقرير Kaspersky (2024) أن قطاع الاتصالات هدف رئيسي للهجمات الإلكترونية في 2024م؛ ويرجع ذلك إلى اهتمام المهاجمين بالبيانات الحساسة، وقد سُجل 284 حادثة أمن سيبراني لكل 10,000 نظام، وبإمكان الهجوم الناجح كشف سجلات ملايين العملاء (مخاطر السرية).

وقد أرجع بعض الباحثين اتساع الفجوة بين المخاطر والضوابط إلى أن التطورات في تكنولوجيا المعلومات لم يرافقتها تطور مماثل في الممارسات والضوابط الأمنية (Muhrtala & Ogundeji, 2013; Tarmidi, 2013; et al.), أو الوصول عن بُعد لأنظمة المعلومات، أو الثغرات الأمنية في البرامج، والأجهزة والضوابط والتنفيذ، وترتبط معظم الثغرات الأمنية في أنظمة المعلومات بالضوابط الأمنية التي لم يتم تطبيقها بقصد أو بدون قصد، أو تم تطبيقها مع وجود بعض نقاط الضعف (JTFTI, 2012)، وقد ناقشت بعض الدراسات الأثر المباشر لمخاطر تكنولوجيا المعلومات في الضوابط الأمنية؛ حيث أشارت دراسة كل من Kumar et al. (2008) Schuessler (2009)، وAl-ghananeem (2014) إلى أن المخاطر تؤثر سلباً في الضوابط الأمنية، وذلك من خلال استغلال الثغرات الأمنية التي تمكن المهاجمين من تجاوز الضوابط الأمنية، والوصول إلى المعلومات وكشفها (مخاطر السرية)، أو تعديلها (مخاطر السلامة)، أو حذفها (مخاطر التوافر). وتعد الثغرات الأمنية في الضوابط الأمنية قضية جوهرية تعاني منها منظمات الأعمال، وتؤثر بشكل سلبي في أنظمة المعلومات المحاسبية، وتؤدي إلى حدوث خسائر مالية، وإضرار بالسمعة، وتوقف النظام، وفقدان إيرادات، ونظراً لأهمية أمن المعلومات في قطاع الاتصالات الذي يُعد العمود الفقري لعالمنا المترابط تم دراسة الضوابط الأمنية لتحقيق هدف الدراسة الحالية المتمثل في قياس أثر مخاطر تكنولوجيا المعلومات في الضوابط الأمنية لدى شركات الاتصالات في صناعة.

الضوابط الأمنية :

تهدف الضوابط الأمنية إلى حماية أصول المنظمة من الوصول غير المصرح به، وتقييد عمليات الوصول المصرح به، والحماية من التعديل غير المشروع، وضمان توافر الأنظمة والخدمات (GAO, 2016)، ويعتمد مستوى الحماية على حساسية وأهمية المعلومات، وتزداد تكاليف الحماية بازدياد مستوى الحماية المطبق؛ لذلك لا بد من الموازنة بين مستوى الحماية وتكاليف تطبيقها (القحطاني, 2015)، ويعتمد اختيار وتطبيق الضوابط الأمنية على تقييم مخاطر نظم المعلومات، فعملية تقييم المخاطر تحدد التهديدات ونقاط الضعف في النظام، والضوابط تحد من المخاطر المحتملة، وتقلل من الخسائر (Yau, 2013).

أولاً: مفهوم الضوابط الأمنية:

يُقصد بالضوابط الأمنية الضوابط الإدارية والتقنية المفروضة على نظام المعلومات لحماية سرية، وسلامة، وتوافر النظام والمعلومات (Committee on National Security Systems [CNSS], 2015)، والضوابط الأمنية مرادف للإجراءات الوقائية والتدابير المضادة. وعرفها المعهد الوطني للمعايير والتكنولوجيا بأنها التدابير المضادة المفروضة على نظام المعلومات التي تهدف إلى: (1) حماية سرية، وسلامة، وتوافر المعلومات التي يتم معالجتها، وتخزينها، ونقلها بواسطة هذه الأنظمة. (2) تلبية مجموعة من متطلبات أمنية محددة. وأيضاً، عرّفها المنظمة الدولية للمعايير (International Organization for Standardization [ISO], 2009) بأنها إدارة المخاطر، بما في ذلك السياسات، والإجراءات، والإرشادات، والممارسات، أو الهياكل التنظيمية التي قد تكون ذات طابع تقني، أو إداري، أو قانوني. وعرفتها دراسة Riad (2009) بأنها التدابير المستخدمة لحماية سرية نظم المعلومات المحاسبية، وسلامتها، وتوافرها.

ولأغراض الدراسة الحالية فإن تعريف الضوابط الأمنية هو: الضوابط التقنية والإدارية اللازمة لحماية سرية المعلومات، وسلامة المعلومات والأنظمة، وتوافرها من المخاطر المختلفة أثناء المعالجة أو التخزين أو النقل.

ثانياً: أهمية الضوابط الأمنية:

تستهدف المخاطر الأمنية سرية المعلومات وسلامتها وتوافرها، وتؤثر هذه المخاطر سلباً في أنظمة الشركات، ويُعد نظام المعلومات عنصراً حيوياً في معظم العمليات التجارية، ومواردها ضرورية لنجاح المنظمة (Swanson et al., 2010). وكما أن هدف الإدارة الأساس هو حماية الموارد التي تدعم عملياتها الحيوية من الوصول غير المصرح به، والحفاظ على سرية المعلومات وسلامتها وتوافرها، وأن تكون الخدمات التي تقدمها هذه الأنظمة قادرة على العمل بفاعلية وباستمرار دون انقطاع، ويتحقق هذا الهدف من خلال تصميم وتنفيذ الضوابط الأمنية (GAO, 2016) التي تبدأ بتحديد هوية مستخدم النظام أو العمليات أو الأجهزة، ثم التحقق من هويتهم كشرط أساسي للسماح لهم بالوصول إلى الموارد في النظام، ثم التحكم بالوصول، وحماية الشبكات، والتشفير (National Institute of Standards and Technology [NIST], 2006; CNSS, 2015).

وأكد تقرير Kaspersky (2024) على أهمية تنفيذ ضوابط الكشف والاستجابة، وإجراء تقييم دوري للاختراق، والاستجابة للحدث عند وقوع هجوم إلكتروني، والاستعانة بخدمات مركز العمليات الأمنية، وتمكين فريق مركز العمليات الأمنية من الحصول على أحدث المعلومات عن التهديدات، وتطوير مهارات فريق الأمن السيبراني لمواجهة أحدث التهديدات، وتطبيق حل أمني لكشف التهديدات المتقدمة بشكل مبكر، وتقديم تدريب للتوعية الأمنية، وتحديث الضوابط الأمنية بانتظام على أساس المخاطر المتغيرة.

وقد أشارت دراسة Choeje et al. (2016) وتقرير PricewaterhouseCoopers (PwC, 2014) إلى أن عوامل النجاح الأكثر أهمية تتمثل في تطبيق المعايير، والامتثال لسياسة الأمن، والتوعية والتدريب، والتخطيط للطوارئ، وتدقيق الأمن، ودعم الأطر القانونية والتنظيمية، وبالتالي فإن منظمات الأعمال تدرك جيداً أهمية الاستثمار في الضوابط الأمنية لحماية أنظمتها من المخاطر، وأولوية الضوابط الأمنية وأهميتها أهمية عالية في منظمات الأعمال، وفي مقدمة أولوياتهم تأمين بيئة تكنولوجيا المعلومات.

ثالثاً: أبعاد الضوابط الأمنية:

الضوابط الأمنية: هي الضوابط الإدارية والتقنية اللازمة لحماية سرية وسلامة وتوافر النظام ومعلوماته؛ وذلك وفقاً للمعهد الوطني للمعايير والتكنولوجيا (NIST)، والمنظمة الدولية للمعايير (ISO, 2009)، ولجنة أنظمة الأمن القومي (CNSS, 2015)، ويتضمن هذا التعريف بُعدين أساسيين لقياس الضوابط الأمنية، وهما:

(1) الضوابط التقنية: وهي التدابير المتخذة لحماية نظام المعلومات من خلال الآليات المدرجة في مكونات الأجهزة والبرامج، كالمصادقة، والتحكم بالوصول، ومكافح البرامج الضارة، وحماية الشبكة، والتشفير (NIST, 2006; Stoneburner et al., 2002).

(2) الضوابط الإدارية: وهي الإجراءات الإدارية المتخذة لحماية أنظمة المعلومات من خلال سياسة الأمن، وخطط الطوارئ، والتوعية والتدريب، وتدقيق الأمن، والتدابير القانونية (Stoneburner et al., 2002; Yau, 2013).

مخاطر تكنولوجيا المعلومات:

تنتج المخاطر الأمنية عن التهديدات التي تستغل الثغرات الموجودة في أصل أو مجموعة من الأصول، وتؤدي إلى إحداث أضرار بالمنظمة (ISO, 2014). ومن أهم القضايا التي تعاني منها منظمات الأعمال حالياً هو استمرار ظهور مخاطر جديدة لم تشهدها المنظمات من قبل، وتتمثل الأضرار الناتجة عن المخاطر في كشف المعلومات، أو تعديلها، أو إتلافها، أو حجب الخدمة (JTFTI, 2012)، وتتراوح الأضرار بين خسائر بسيطة إلى تدمير نظام بالكامل (Jouini et al., 2014).

أولاً: مفهوم مخاطر تكنولوجيا المعلومات:

عرّف المعهد الوطني للمعايير والتكنولوجيا (JTFTI, 2012) مخاطر أمن المعلومات بأنها تلك المخاطر التي تنشأ عن فقدان سرية المعلومات، أو سلامتها، أو توافرها، وتنعكس الآثار السلبية المحتملة على عمليات وأصول المنظمة، وأيضاً عرّف المعهد الوطني للمعايير والتكنولوجيا (JTFTI, 2012) مخاطر تكنولوجيا المعلومات بأنها الأثر المحتمل على الأعمال من مصدر تهديد معين يستغل ثغرات معينة في تكنولوجيا المعلومات، وتنشأ مخاطر تكنولوجيا المعلومات عن الآتي: (1) كشف المعلومات غير المصرح بها، أو تعديلها، أو إتلافها. (2) الأخطاء أو الإهمال. (3) تعطل تكنولوجيا المعلومات بسبب الكوارث الطبيعية أو كوارث من صنع الإنسان.

ولأغراض الدراسة الحالية فإنه يمكن تعريف مخاطر تكنولوجيا المعلومات بأنها: المخاطر الناتجة عن كشف المعلومات (فقدان السرية)، أو تعديل المعلومات أو إتلافها (فقدان السلامة)، أو توقف النظام والخدمات (فقدان التوافر)، والتي تؤثر سلباً في عمليات وأصول المنظمة.

ثانياً: أبعاد مخاطر تكنولوجيا المعلومات:

كما أشرنا سابقاً إلى مفهوم مخاطر تكنولوجيا المعلومات بأنها: تلك المخاطر التي تنشأ عن فقدان سرية المعلومات، أو فقدان سلامتها، أو فقدان توافرها، وذلك وفقاً للمعهد الوطني للمعايير والتكنولوجيا (JTFTI, 2012)، ودراسة Azees et al. (2016)، ودراسة Gordon et al. (2011). ويتضمن هذا التعريف ثلاثة أبعاد، وهي: (1) المخاطر المتعلقة بالسرية: وتعني الكشف أو الوصول غير المصرح به للمعلومات السرية (Gordon et al., 2011). (2) المخاطر المتعلقة بالسلامة: وتعني التعديل أو الإتلاف غير المصرح به للمعلومات أو الأنظمة (Rhodes-Ousley, 2013). (3) المخاطر المتعلقة بالتوافر: وتعني منع المستخدمين المخولين من الوصول إلى المعلومات أو نظام المعلومات عند الطلب (Gordon et al., 2011; Rhodes-Ousley, 2013). (4) وقد تم إضافة المخاطر العامة أو المشتركة كبعد 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 العامة التي تستهدف عنصرين أو أكثر من عناصر أمن المعلومات: (السرية، والسلامة، والتوافر) في آن واحد.

النظريات المفسرة لمتغيرات الدراسة:

أولاً: نظرية الردع العام:

تعاني أنظمة المعلومات من أنواع معينة من المخاطر، وتكمن المشكلة في عدم إدراك المعنيين لمجموعة كاملة من الضوابط الأمنية التي يمكن اتخاذها للحد من المخاطر، ويمكن الحد من المخاطر في حال إدراك النطاق

الكامل للضوابط الأمنية المتاحة، وتنفيذ أكثرها فاعلية. وهناك نظريات سلوكية تقدم نظرة حول كيفية التعامل مع المخاطر، مثل نظرية الردع العام التي تركز على العقوبات التي تؤثر في الآخرين، حيث إن العقوبات تعمل كمثبطات للأفعال غير المشروعة (Straub & Welke, 1998)، فعندما تكون مخاطر العقاب مرتفعة، والعقوبات على الانتهاكات شديدة، تتنبأ النظرية بردع الجناة المحتملين عن ارتكاب الأفعال غير المشروعة (Straub, 1990)، وتفترض النظرية إجراءات عامة تقلل من المخاطر بشكل مباشر أو غير مباشر من خلال استخدام الضوابط الأمنية (Straub & Welke, 1998).

وقد توسعت دراسة D'Arcy et al. (2009) في نظرية الردع العام؛ حيث تفترض أن وعي المستخدم بالضوابط الأمنية يؤثر بشكل مباشر وغير مباشر في نوايا المستخدمين المتعلقة بإساءة استخدام أنظمة المعلومات من خلال إدراك المستخدمين للعقوبة، وأيضاً توسعت دراسة Schuessler (2009) في وجهات النظر المفاهيمية لنظرية الردع العام لتشمل المخاطر غير البشرية (الكوارث الطبيعية، والإخفاق التقني)، ويساعد هذا التوسع في التخطيط الوقائي للحد من المخاطر.

وقد تم تصنيف التدابير المضادة (الضوابط الأمنية) إلى أربع فئات: (الردع، والوقاية، والكشف، والمعالجة)، ويساعد هذا التصنيف في إيجاد بدائل أمنية تقدم للممارسين منظورا نظريا لتنفيذ التدابير المضادة (Straub & Welke, 1998)، وقد صنفت الدراسة الحالية الضوابط الأمنية إلى ضوابط تقنية وإدارية لم يتم تناول هذا التصنيف من قبل، وقد أشار إلى هذا التصنيف كإطار نظري كل من لجنة أنظمة الأمن القومي، والمعهد الوطني للمعايير والتكنولوجيا، وما يميز هذا التصنيف عن التصنيفات السابقة هو عدم تداخل عناصر الضوابط التقنية والإدارية فيما بينهما إلى حد ما، وكل فئة تختلف عناصرها عن عناصر الفئة الأخرى، وقد اعتمدت هذه الدراسة على هذه النظرية كإطار نظري يمكن المنظمة من استخدام الضوابط الأمنية المتاحة في الحفاظ على الأنظمة، وما يبرر الأخذ بهذه نظرية في الدراسة الحالية هو إمكانية تطبيقها على أنظمة المعلومات.

ثانياً: نظرية أمن المعلومات:

أدى تطور مجتمع المعلومات إلى زيادة المخاطر، وعندما تصبح المعلومات سلعة أساسية في عالم اليوم، فإن هناك حاجة ملحة إلى حمايتها، وهذا يتطلب إطاراً نظرياً للحفاظ على المعلومات، وقد تم بالفعل وضع أسس نظرية شاملة لأمن المعلومات، بحيث يتم بموجبها تنفيذ الحماية على أساس علمي ومنهجي متين (Malyuk & Miloslavskaya, 2014)، وتشير دراسة Horne et al. (2016) إلى أن هدف أمن المعلومات ببساطة هو خلق الموارد، وتنص هذه النظرية على أن الدافع وراء كل المحاولات التي تقوم بها المنظمات لتأمين المعلومات من المخاطر هو خلق الموارد التي يمكن استخدامها لاحقاً في تحسين الأداء، وقد نشأت هذه النظرية في مجال نظم المعلومات، وبُنيت بالكامل من المفاهيم المتعلقة بالمعلومات، حيث إن أمن المعلومات هو ظاهرة تقع ضمن نطاق نظم المعلومات، وتعد هذه النظرية تفسيرية وليست تنبؤية، فهي تقدم تفسيرات سببية محددة، ومقترحات قابلة للاختبار، وبيانات وصفية، ويمكن استخدام هذه النظرية في تفسير الدوافع وراء الجهود الرامية إلى حماية المعلومات المستخدمة من قبل الأفراد، والمنظمات، والدول، وتنص هذه النظرية على أن تطبيق الضوابط يؤدي إلى تحويل المعلومات إلى موارد، وأن تطبيق الضوابط أيضاً يزيد من احتمالية تحويل المعلومات إلى موارد (Horne et al., 2016).

وكما أن التهديدات المختلفة تستغل نقاط الضعف التي تؤثر سلباً في البنية التحتية، فقد يؤدي الاختراق إلى توقف العمليات، وفقدان إيرادات، وفقدان الثقة، وبالتالي التآكل المحتمل للميزة التنافسية (Von Solms & van Niekerk, 2013). وتؤدي المخاطر إلى انتهاك سلامة المعلومات وسريتها وتوافرها، فبعض المعلومات محمية من قبل الضوابط لإنتاج مورد يمكن الاعتماد عليه، وأن جميع المعلومات التي يتعين استخدامها يجب أن تكون محمية (Horne et al., 2016)، ويساعد تطبيق الضوابط الأمنية في حماية المعلومات من المخاطر المختلفة، ومنع وكشف الهجمات، والتعافي منها (Posthumus & von Solms, 2004)، ويؤدي تطبيق الضوابط الأمنية إلى حماية المعلومات من المخاطر، ويمكن أيضاً تطبيق

الضوابط التقنية والإدارية لحماية المعلومات أثناء التخزين أو المعالجة أو النقل (Horne et al., 2016).

الدراسات السابقة:

تناولت بعض الدراسات تأثيرات أحادية الاتجاه، مثل دراسة أثر المخاطر في الضوابط الأمنية، وتناول آخرون التأثيرات المتبادلة؛ حيث أشارت دراسة Schuessler (2009) إلى أن المخاطر تؤثر في التدابير المضادة؛ (الوقائية، والردع، والكشف، والمعالجة) المستخدمة في حماية أنظمة المعلومات، وأن التدابير المضادة؛ (الوقائية، والمعالجة) تؤثر في المخاطر، بينما التدابير المضادة؛ (الردع، والكشف) لا تؤثر في المخاطر، فكلما زادت المخاطر التي تواجهها المنظمة يتم تنفيذ كل نوع من أنواع التدابير المضادة.

وقد أظهرت دراسة Straub (1987) أن العلاقة السببية قوية بين جهود الردع وانخفاض الضرر، وأن التدابير الوقائية أداة فاعلة في الحد من إساءة استخدام الحاسوب، وأن المخاطر تدفع المنظمات إلى استخدام التدابير المضادة، وتوصلت دراسة Al-ghananeem (2014) إلى أن المخاطر تؤثر سلباً في ضمان أمن المعلومات، وذكرت دراسة Riad (2009) أن الضوابط الأمنية لها تأثير كبير في العديد من المخاطر، وتشير دراسة Kumar et al. (2008) إلى أن التدابير المضادة تقلل من التأثيرات السلبية للهجمات المختلفة، وتقلل من وقت الاسترداد. وذكرت دراسة D'Arcy et al. (2009) أن مستوى وعي الموظفين العالي بالضوابط يقلل من نوايا إساءة استخدام التكنولوجيا، وأن القوانين والعقوبات يمكنها شتي الأفراد عن الانخراط في السلوك غير المشروع، وأن سياسة الأمن الفاعلة تردع إساءة استخدام الأنظمة، وذكرت دراسة Al-shaibany et al. (2023) أن المخاطر التي تواجه أصول القطاع المصرفي اليمني كالهجمات المختلفة هي التي تستهدف خصوصية العملاء، وسرية البيانات، وسلامتها، وتوافرها.

وتناول آخرون الثغرات الأمنية أو نقاط الضعف في الضوابط الأمنية التي تستغلها التهديدات؛ حيث ذكر تقرير CERT Australia (2014) أن الشبكة الداخلية تتضمن مجموعة من نقاط الضعف، بعضها في المصادقة، مما سهل عملية الوصول غير المصرح به إلى الشبكة. وكشف تقرير Symantec Corporation (2016) عن حدوث هجمات اعتمدت على الهندسة الاجتماعية المتطورة أدت إلى تجاوز أنظمة المصادقة المستندة على معايير، وكشفت دراسة Medina et al. (2013) عن عمليات احتيال تتمثل في سرقة (36) مليون يورو من عميل من عملاء المصارف في هولندا وأسبانيا وألمانيا؛ حيث استهدف المهاجمون أجهزة الحواسيب الشخصية، وأجهزة الهواتف النقالة الخاصة بالمستخدمين من خلال السيطرة على المصادقة المستندة على معايير، وذكر تقرير GAO (2015) أن الوكالات الفدرالية عانت من جوانب ضعف في التحكم بالوصول، والفصل في المهام، وخطة استمرارية العمل، وبالتالي تستغل التهديدات جوانب الضعف في الضوابط الأمنية للوصول لأنظمة المعلومات. وأشار تقرير Office of Management and Budget (OMB, 2016) إلى أن هجمات الهندسة الاجتماعية، والاصطياد الإلكتروني، والشفرات الخبيثة يمكن دفعها من خلال استخدام قدرات بطاقة التحقق من صحة الهوية الشخصية (Personal Identity Verification [PIV])، وتدريب المستخدمين، أيضاً، يمكن ردع الاستخدام غير السليم، وانتهاك السياسة، والوصول غير المصرح به من خلال المصادقة القوية.

وأكدت دراسة Department for Business, Innovation & Skills (2013) أن هناك علاقة واضحة بين الأخطاء التقنية والبشرية، وبين وعي الموظفين بالأمن، وأن وعي الموظفين يُحد من تلك المخاطر، وذكر تقرير Verizon أن 86% من عمليات الاختراق استغلت ثغرات في ضوابط التحقق من الهوية والتحكم بالوصول (Verizon, 2025)، وأكدت دراسة Nhan et al. (2025) أن نقص معرفة الموظفين بأمن المعلومات يتسبب في حدوث ثغرات أمنية، مثل تنزيل برامج ضارة، أو استخدام كلمات مرور ضعيفة.

مشكلة الدراسة:

تتمثل مشكلة الدراسة في الثغرات الأمنية أو جوانب القصور في الضوابط الأمنية التي تستغلها التهديدات، وتسبب أضراراً لشركات الاتصالات في اليمن على الرغم من استخدام الضوابط الأمنية في حماية أنظمة المعلومات من مخاطر تكنولوجيا المعلومات؛ وقد أشارت دراسة الربيدي (2010) إلى أن إدارة البنوك في اليمن تقوم بحماية معلوماتها غالباً من خلال الرقابة على الوصول المادي، ونظم للصلاحيات، والرقابة على النسخ الاحتياطي، ومكافح الفيروسات، والتشفير، وتوصلت دراسة فاضل (2018) إلى أن البنوك التجارية في اليمن تنفذ آليات الحماية بشكل كاف وفعال، وتتمثل آليات الحماية المنفذة في: أمن تعديل وتطوير النظم، يليها أمن المدخلات، ثم أمن الوسائط، وأمن المخرجات، وأيضاً أشارت إلى أن آليات الحماية لها تأثير إيجابي في ضمان أمن نظم المعلومات الحاسوبية من المخاطر، وذكر تقرير International Telecommunication Union (ITU, 2015) أن التحقيق في الجرائم السيبرانية، وملاحقة مرتكبيها، وفرض عقوبات على الجناة تحد من مخاطر تكنولوجيا المعلومات.

وقد أصدر البرلمان اليمني قانون رقم (40) لسنة 2006م بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية (2006) بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية، وهو يهدف إلى تعزيز الإشراف والرقابة، ويسري على التعاملات الإلكترونية، وأيضاً أصدر البرلمان اليمني قانون رقم (13) لسنة 2012م بشأن حق الحصول على المعلومات (2012) الذي يتضمن حماية نظم وشبكات المعلومات من المخاطر.

وعلى الرغم من استخدام الضوابط الأمنية في حماية أنظمة المعلومات من المخاطر فإن هناك جوانب قصور وثغرات أمنية تستغل في تنفيذ الهجمات؛ حيث وجدت دراسة Schuessler (2009) أن الضوابط الأمنية يمكنها الحد من المخاطر، وليس منع جميع المخاطر، وقد أشارت نتائج الدراسة الاستطلاعية التي قام بها الباحث إلى وجود مخاطر تهدد أمن نظم المعلومات الحاسوبية في شركات الاتصالات مجتمع الدراسة، والمتمثلة في التعديل غير المصرح به لحد ائتمان المشتركين، وتوقف النظام، وإجراء مكالمات مجانية، واختلاف زمن المكالمات في السنترال عن تكاليفها في نظام الفوترة، وعدم إجراء التسويات الدورية للجزء المستنفذ من كروت الخدش والاعتراف به كإيراد، وعدم إنشاء بعض حسابات المشتركين في نظام الفوترة، والتقادم التكنولوجي للأجهزة والبرامج، والحروب، والانعدام الكلي للطاقة العمومية.

وقد يؤدي استغلال الثغرات في الضوابط الأمنية إلى خسائر مالية كبيرة وخسائر غير مباشرة، مثل الإضرار بالسمعة والعلامة التجارية، وتوقف النظام، وفقدان إيرادات؛ حيث كشف تقرير Reuters (2015) عن استهداف برامج التجسس الإلكتروني قطاع الاتصالات في اليمن، وذلك من خلال وضع تعليمات برمجية في محركات الأقراص المنتجة من قبل كبرى الشركات الإلكترونية في الولايات المتحدة، وأشارت عدن الغد (2014) إلى حدوث خلل فني أثناء الصيانة في إحدى شركات الاتصالات العاملة في اليمن؛ مما أدى إلى توقف خدمة الاتصالات لساعات، وتسبب ذلك في فقدان إيرادات، وعبر المشتركون عن استيائهم من توقف الخدمة التي عطلت أعمال الكثير منهم، وكشف تقرير وزارة الاتصالات وتقنية المعلومات (2020) عن خسائر قطاع الاتصالات في اليمن من مارس 2015م إلى مارس 2020م بمقدار 4.1 مليار دولار ناتجة عن تدمير البنية التحتية، وقد أثرت الحرب وانقطاع الطاقة سلباً في سلامة المعلومات وخدمات الاتصالات وتوافرها، وتسبب انقطاع الكابل البحري في توقف الخدمات وحدوث شلل في المعاملات المالية. وقد وجدت دراسة الربيدي (2010) قصوراً في الضوابط الأمنية المستخدمة في البنوك، ومنها: قصور في النسخ الاحتياطي للبيانات، والتخطيط للطوارئ، والرقابة الآلية، ومراجعة مخرجات النظام الحاسبي، والسياسة الأمنية لحماية الأجهزة والبرامج والبيانات، وتواجه العمليات المصرفية الإلكترونية مخاطر في الوصول المصرح به، وخصوصية العملاء، وسلامة تجهيز وتخزين البيانات. وقد أشارت دراسة فاضل (2018) إلى أن البنوك التجارية في اليمن تنفذ آليات الحماية بشكل كاف وفعال، ولكنها ليست منفذة بالشكل الأمثل، وتحتاج إلى تطوير وتحديث مستمر، حيث تواجه البنوك مخاطر تهدد سرية

المعلومات، وسلامة وتكامل المعلومات، وخصوصية العملاء، وتوافر الأنظمة، وذكرت (الثورة نت، 2025) أن إعادة تقييم الثغرات الأمنية المحتملة تعتمد على الموظف أكثر من الاعتماد على برامج وأنظمة الحماية، والتأكيد على أهمية تعزيز الثقافة الأمنية، ورفع مستوى الوعي في مجال أمن المعلومات، وذكرت دراسة Al-shaibany et al. (2023) المخاطر التي تواجه أصول القطاع المصرفي اليمني، كالهجمات المختلفة التي تستهدف خصوصية العملاء، وسرية البيانات، وسلامتها، وتوافرها.

وقد أشارت بعض التقارير (ITU, 2015, 2017, 2019, 2021; National Cyber Security Index, 2020) إلى تدني مستوى الأمن السيبراني في اليمن الناتج عن جوانب قصور في القوانين، واللوائح، وفريق الاستجابة لحالات الطوارئ والحوادث، والسياسات العامة، والاستراتيجيات الوطنية، والمعايير، وبرامج التوعية والتدريب، وأشار تقرير ITU (2024) إلى تدني مستوى الأمن في اليمن فيما يتعلق بالتدابير القانونية والتقنية والتنظيمية، وتنمية القدرات، والتعاون، وأكد نائب رئيس الوزراء وزير الاتصالات (سبانت، 2014) في المؤتمر الأول لأمن المعلومات أن هناك قصورا في التشريع اليمني فيما يتعلق بحماية خصوصيات وممتلكات الناس، وأيضا أكد على أهمية إنشاء مركز وطني لأمن المعلومات؛ بغرض الاستجابة لحوادث أمن المعلومات، ولاحتوائها، وتجنبها مستقبلا.

ووفقا لنظرية الردع العام (Straub & Welke, 1998) التي تفترض أن الإجراءات العامة تقلل من المخاطر بشكل مباشر أو غير مباشر من خلال استخدام الضوابط الأمنية، واستنادا إلى نظرية أمن المعلومات (Horne et al., 2016) التي تنص على أن الدافع وراء كل المحاولات التي تقوم بها المنظمات لتأمين معلوماتها من المخاطر هو خلق الموارد التي يمكن استخدامها لاحقا في تحسين الأداء، وأيضا تنص هذه النظرية على أن تطبيق الضوابط الأمنية يؤدي إلى تحويل المعلومات إلى موارد، وأن العلاقة بين الضوابط والمخاطر سلبية، وقد توسعت الدراسة الحالية في نظرية الردع العام لتشمل المخاطر التي تستهدف السرية، والسلامة، والتوافر، والعامة، ويمكن منع تلك المخاطر أو الحد منها في حال إدراك النطاق الكامل للضوابط التقنية والإدارية، وتنفيذ أكثرها فاعلية.

وبالتالي، تسعى الدراسة الحالية إلى الإسهام في تحديد المخاطر، ومنعها أو الحد من آثارها السلبية، ومعالجة جوانب القصور والثغرات في أنظمة الحماية لدى شركات الاتصالات مجتمع الدراسة، وذلك من خلال تنفيذ وتحديث الضوابط الأمنية بما في ذلك تطبيق المعايير المهنية، والالتزام بالسياسة الأمنية، وتنفيذ برامج التوعية، وتدقيق الأمن، ودعم الأطر القانونية والتنظيمية، والاستفادة من الممارسات المثلى في تعزيز الأمن، ومواكبة التطورات التكنولوجية.

أسئلة الدراسة:

بناء على مشكلة الدراسة يمكن صياغة السؤال الآتي:

السؤال الرئيس: هل تؤثر مخاطر تكنولوجيا المعلومات في الضوابط الأمنية لدى شركات الاتصالات في صنعاء؟ وسيتم الإجابة عن هذا السؤال من خلال الإجابة عن الأسئلة الفرعية الآتية:

1. هل تؤثر المخاطر المتعلقة بالسرية في الضوابط التقنية لدى شركات الاتصالات في صنعاء؟
2. هل تؤثر المخاطر المتعلقة بالسرية في الضوابط الإدارية لدى شركات الاتصالات في صنعاء؟
3. هل تؤثر المخاطر المتعلقة بالسلامة في الضوابط التقنية لدى شركات الاتصالات في صنعاء؟
4. هل تؤثر المخاطر المتعلقة بالسلامة في الضوابط الإدارية لدى شركات الاتصالات في صنعاء؟
5. هل تؤثر المخاطر المتعلقة بالتوافر في الضوابط التقنية لدى شركات الاتصالات في صنعاء؟
6. هل تؤثر المخاطر المتعلقة بالتوافر في الضوابط الإدارية لدى شركات الاتصالات في صنعاء؟
7. هل تؤثر المخاطر العامة (المشتركة) في الضوابط التقنية لدى شركات الاتصالات في صنعاء؟
8. هل تؤثر المخاطر العامة (المشتركة) في الضوابط الإدارية لدى شركات الاتصالات في صنعاء؟

أهداف الدراسة:

بناء على أسئلة الدراسة تم صياغة مجموعة من الأهداف التي تسعى الدراسة الحالية إلى تحقيقها، وهي:

الهدف الرئيس: قياس أثر مخاطر تكنولوجيا المعلومات في الضوابط الأمنية لدى شركات الاتصالات في صنعاء. ويتفرع هذا الهدف إلى مجموعة من الأهداف الفرعية الآتية:

1. قياس أثر المخاطر المتعلقة بالسرية في الضوابط التقنية لدى شركات الاتصالات في صنعاء.
2. قياس أثر المخاطر المتعلقة بالسرية في الضوابط الإدارية لدى شركات الاتصالات في صنعاء.
3. قياس أثر المخاطر المتعلقة بالسلامة في الضوابط التقنية لدى شركات الاتصالات في صنعاء.
4. قياس أثر المخاطر المتعلقة بالسلامة في الضوابط الإدارية لدى شركات الاتصالات في صنعاء.
5. قياس أثر المخاطر المتعلقة بالتوافر في الضوابط التقنية لدى شركات الاتصالات في صنعاء.
6. قياس أثر المخاطر المتعلقة بالتوافر في الضوابط الإدارية لدى شركات الاتصالات في صنعاء.
7. قياس أثر المخاطر العامة (المشتركة) في الضوابط التقنية لدى شركات الاتصالات في صنعاء.
8. قياس أثر المخاطر العامة (المشتركة) في الضوابط الإدارية لدى شركات الاتصالات في صنعاء.

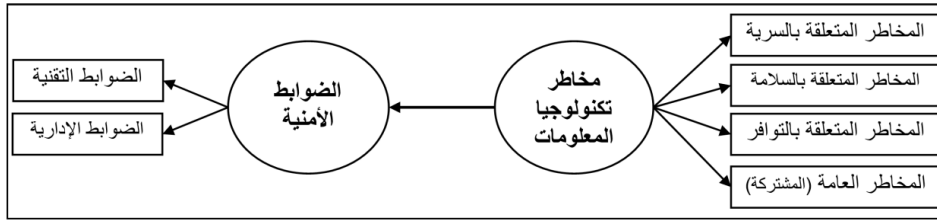
أهمية الدراسة:

تتمثل أهمية الدراسة الحالية في الآتي:

1. تركيز الدراسة الحالية على الضوابط الأمنية في شركات الاتصالات في صنعاء؛ نظرا لأهمية الضوابط الأمنية في حماية موارد القطاع من الوصول غير المصرح به، ومنع أو كشف التعديل غير المصرح به، وتوافر الخدمات للمخوليين.
2. تناولت الدراسة الحالية مخاطر تكنولوجيا المعلومات في شركات الاتصالات مجتمع الدراسة؛ كون هذا القطاع هدفا للمهاجمين الذين يستهدفون سرية المعلومات وخصوصية العملاء، وسلامة المعلومات والأنظمة، وتوافرها.
3. تسهم الدراسة الحالية في دراسة الضوابط التقنية والضوابط الإدارية كأبعاد جديدة للضوابط الأمنية لم يسبق دراستهما من قبل، وأضافت الدراسة الحالية بُعدا جديدا خاصا بالمخاطر العامة أو المشتركة.
4. تطوير أداة لقياس أثر مخاطر تكنولوجيا المعلومات في الضوابط الأمنية لدى شركات الاتصالات مجتمع الدراسة وفقا لنظرية الردع العام، ونظرية أمن المعلومات التي تفسر العلاقة بين متغيرات الدراسة.
5. إمكانية استفادة مجلس الإدارة والإدارة التنفيذية في شركات الاتصالات داخل اليمن وخارجها في قياس درجة مخاطر تكنولوجيا المعلومات ومدى استخدام الضوابط الأمنية.
6. إمكانية استفادة كل من إدارة تكنولوجيا المعلومات، وإدارة التدقيق الفني، وإدارة الرقابة والتحكم، وإدارة تشغيل الشبكة والإنترنت في شركات الاتصالات مجتمع الدراسة، وذلك من خلال تنفيذ الضوابط الأمنية الملائمة، وتلافي جوانب الضعف والقصور في الضوابط الأمنية.
7. بناء نموذج معرفي جديد يستند على الدراسات السابقة والنظريات العلمية المفسرة للعلاقة بين متغيرات الدراسة.

النموذج المعرفي:

بناء على الخلفية النظرية والأدب السابق، يُمكننا بناء النموذج المعرفي للدراسة الحالية كما هو موضح في الشكل (1).



شكل (1): النموذج المفاهيمي للدراسة

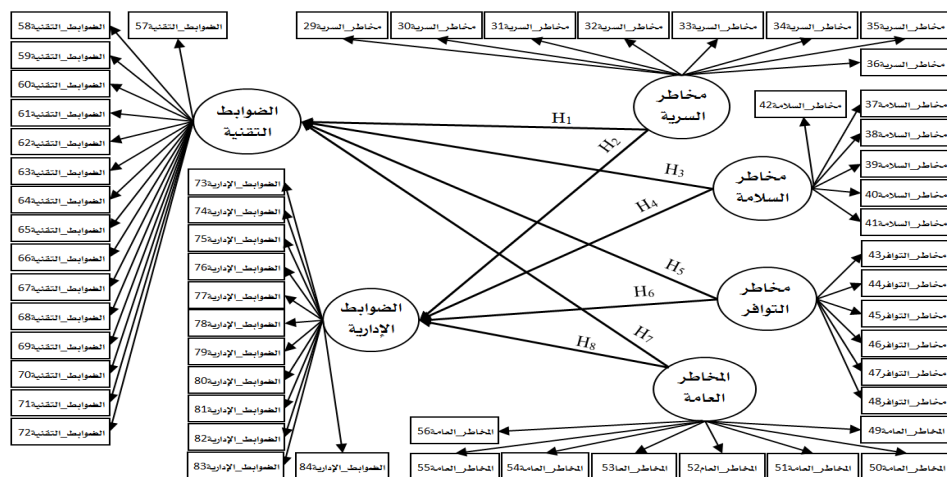
تطوير فرضيات الدراسة:

بناء على ما سبق من نظريات علمية (Horne et al., 2016; Straub & Welke, 1998)، ودراسة كل من (Kumar et al., 2008)، و (D'Arcy et al., 2009)، و (Schuessler, 2009)، و (Riad, 2009)، و (Tarmidi et al., 2013)، و (Al-ghananeem, 2014)، والتي تشير إلى أن المخاطر تؤثر سلباً في الضوابط الأمنية، وذلك من خلال استغلال الثغرات الأمنية أو القصور في تنفيذ الضوابط وتحديثها؛ حيث أشار NIST (2006) إلى أن الثغرات الأمنية قد توجد في خطط الطوارئ، والنسخ الاحتياطي، والمصادقة والتشفير، والتقنيات المتقدمة، وقصور في الجوانب التشريعية والتنظيمية المتعلقة بأمن المعلومات، وتؤكد تلك النظريات والدراسات على العلاقة السلبية بين المخاطر والضوابط الأمنية، وبالتالي يمكن تطوير الفرضية الرئيسية لهذه الدراسة على النحو الآتي:

H: تؤثر مخاطر تكنولوجيا المعلومات سلباً في الضوابط الأمنية لدى شركات الاتصالات في صناعة، والشكل (1) يوضح مسار هذه الفرضية، ويتفرع من هذه الفرضية ثمان فرضيات فرعية تتمثل بالآتي:

- H1: تؤثر المخاطر المتعلقة بالسرية سلباً في الضوابط التقنية لدى شركات الاتصالات في صناعة.
- H2: تؤثر المخاطر المتعلقة بالسرية سلباً في الضوابط الإدارية لدى شركات الاتصالات في صناعة.
- H3: تؤثر المخاطر المتعلقة بالسلامة سلباً في الضوابط التقنية لدى شركات الاتصالات في صناعة.
- H4: تؤثر المخاطر المتعلقة بالسلامة سلباً في الضوابط الإدارية لدى شركات الاتصالات في صناعة.
- H5: تؤثر المخاطر المتعلقة بالتوافر سلباً في الضوابط التقنية لدى شركات الاتصالات في صناعة.
- H6: تؤثر المخاطر المتعلقة بالتوافر سلباً في الضوابط الإدارية لدى شركات الاتصالات في صناعة.
- H7: تؤثر المخاطر العامة (المشتركة) سلباً في الضوابط التقنية لدى شركات الاتصالات في صناعة.
- H8: تؤثر المخاطر العامة (المشتركة) سلباً في الضوابط الإدارية لدى شركات الاتصالات في صناعة.

ويوضح الشكل (2) مسار الفرضيات الفرعية.



شكل (2): مسار الفرضيات الفرعية

منهجية الدراسة وإجراءاتها:

منهج الدراسة:

اعتمدت الدراسة الحالية على المنهج التحليلي، وتم استخدام أساليب الإحصاء الاستدلالي لتحقيق هدف الدراسة المتمثل في قياس أثر مخاطر تكنولوجيا المعلومات في الضوابط الأمنية لدى شركات الاتصالات بصنعا.

مجتمع الدراسة:

استهدفت الدراسة الحالية شركات الاتصالات في صنعا، والذي يتضمن ست شركات: (سبأفون، تيليمن، يمن موبايل، إم تي إن، يمن نت، واي)، والمؤسسة العامة للاتصالات وفقا لأسلوب الحصر الشامل، ويكون مجتمع الدراسة من (356) عنصرا يشمل: المدراء، ورؤساء الأقسام، والمشرفين، والمختصين في إدارة تكنولوجيا المعلومات، وإدارة التدقيق الفني، وإدارة الرقابة والتحكم، وإدارة تشغيل الشبكة والإنترنت الموجودة في العاصمة صنعا، وقد تم استبعاد فروعها في بقية المحافظات؛ كون الكوادر الفنية ذات المهارات العالية تتواجد في المراكز الرئيسية، وقد تم جمع المعلومات عن مجتمع الدراسة من خلال النزول الميداني، والمختصين في إدارة الموارد البشرية، ومواقع الويب، وكتاب الإحصاء السنوي، وتم اختيار شركات الاتصالات مجتمعا للدراسة؛ نظرا لاعتمادها على تكنولوجيا المعلومات بشكل كبير، واستخدام الضوابط الأمنية في حماية سرية المعلومات، وسلامتها، وتوافرها من المخاطر. ويوضح الجدول (1) المجتمع المستهدف ونسبة الاستجابة.

جدول (1): المجتمع المستهدف ونسبة الاستجابة

رمز م الشركة أو المؤسسة	الاستبيان	الاستبيان الصالح للتحليل في إدارة كل من					نسبة إجمالي الاستجابة	نسبة الاستجابة
		الموزع	المسترد	الصالح للتحليل	تكنولوجيا المعلومات	التدقيق الفني	الرقابة والتحكم	تشغيل الشبكة والإنترنت
1 A	92	81	79	28	3	7	41	79
2 B	50	25	24	9	2	3	10	24
3 C	66	54	52	24	4	5	19	52

جدول (1): يتبع

م	رمز الشركة أو المؤسسة	الموزع	المسترد	الصالح للتحليل	تكنولوجيا المعلومات	التدقيق الفني	الرقابة والتحكم	تشغيل الشبكة والإنترنت	الاستبيان الصالح للتحليل في إدارة كل من	
									إجمالي	نسبة الاستجابة
4	D	30	22	22	12	2	2	6	22	73 %
5	E	52	16	16	5	1	0	10	16	31 %
6	F	45	20	17	8	0	4	5	17	38 %
7	G	21	8	8	4	0	0	4	8	38 %
	الإجمالي	356	226	218	90	12	21	95	218	61 %
	النسبة	100 %	63 %	61 %	25.28 %	3.37 %	5.90 %	26.69 %		

ملاحظة: تم ترميز مجتمع الدراسة بناء على رغبة بعض الإدارات في القطاع.

وقد تم توزيع (356) استبانة على جميع عناصر المجتمع من خلال النزول الميداني، والموارد البشرية، وتم استرداد (226) استبانة بنسبة 63%، والصالح للتحليل (218) استبانة بنسبة 61% من الاستبانات الموزعة، ونسبة الاستبانات غير المستردة 37%؛ ويعود ارتفاع نسبة عدم الاستجابة إلى قلق بعض الموظفين من تقديم المعلومات اللازمة للدراسة؛ كونها باعتقادهم سرية وتؤثر سلباً على شركتهم؛ لذلك تم حجز (130) استبانة من قبل بعض الإدارات.

وحدة التحليل:

تتمثل وحدة التحليل في الدراسة الحالية بالمنظمة (المؤسسة العامة للاتصالات + ست شركات اتصالات) وعددها سبع؛ كون المتغير التابع (الضوابط الأمنية ببعديها) والمتغير المستقل (مخاطر تكنولوجيا المعلومات بأبعادها الأربعة) تقاس على مستوى المنظمة، وتعد الإدارات الأربع هي المعنية بالإجابة عن فقرات الاستبانة.

تطوير أداء الدراسة:

تم تطوير أداء الدراسة المستخدمة في جمع البيانات المتعلقة بالضوابط الأمنية (المتغير التابع) بالاعتماد على الجانب النظري، ودراسة كل من Abu-Hayale وWhitman (2004)، وKhadra (2006)، وRiad (2009)، وSchuessler (2009)، وتم قياس الضوابط الأمنية من خلال بُعد الضوابط التقنية الذي يتضمن 16 فقرة، وبُعد الضوابط الإدارية الذي يتضمن 12 فقرة، وأيضاً تم تطوير قائمة مخاطر تكنولوجيا المعلومات (المتغير المستقل) بالاعتماد على الجانب النظري، ودراسة كل من Abu-Hayale وRiad (1992)، وSchuessler (2009)، وتم قياس مخاطر تكنولوجيا المعلومات من خلال بُعد المخاطر المتعلقة بالسرية الذي يتضمن 8 فقرات، وبُعد المخاطر المتعلقة بالسلامة الذي يتضمن 6 فقرات، وبُعد مخاطر التوافر الذي يتضمن 6 فقرات، وبُعد المخاطر العامة الذي يتضمن 8 فقرات.

وقد تضمنت الاستبانة محورين رئيسيين، المحور الأول: تضمن جمع بيانات عن مدى استخدام الضوابط الأمنية في شركات الاتصالات. والمحور الثاني: تضمن جمع بيانات عن درجة مخاطر تكنولوجيا المعلومات في شركات الاتصالات مجتمع الدراسة، وتم استخدام مقياس ليكرت السباعي للضوابط الأمنية وفقاً لدراسة Loch et al. (1992)، ودراسة Schuessler (2009)؛ حيث إن (7) إلى "تستخدم على نطاق واسع"، وتعني أن استخدام الضوابط الأمنية في حماية الأنظمة من المخاطر في شركات الاتصالات مرتفع جداً، ويشير (1) إلى "قليلة الاستخدام"، وتعني أن استخدام الضوابط الأمنية في حماية الأنظمة من المخاطر في شركات الاتصالات منخفض جداً.

وتم استخدام مقياس ليكرت السباعي لمخاطر تكنولوجيا المعلومات وفقاً لدراسة Loch et al. (1992)، ودراسة Schuessler (2009)؛ حيث تشير (7) إلى "أعلى درجة"، وتعني أن المخاطر التي تواجه الأنظمة في شركات الاتصالات مرتفعة جداً، ويشير (1) إلى "أقل درجة"، وتعني أن المخاطر التي تواجه الأنظمة في شركات الاتصالات منخفضة جداً.

اختبار صدق المحتوى للأداة:

تم عرض الاستبانة على عدد من المحكمين المتخصصين للتأكد من أن فقرات الاستبانة شاملة وكافية لقياس مدى استخدام الضوابط الأمنية ودرجة مخاطر تكنولوجيا المعلومات في شركات الاتصالات مجتمع الدراسة، وقد أبدى المحكمون آراءهم وقدموا مقترحاتهم حول تعديل بعض الفقرات، أو إعادة صياغتها، أو إضافة فقرات جديدة لتحسين الاستبانة، وقد تم إجراء التعديلات اللازمة بناءً على مقترحات المحكمين.

اختبار صدق وثبات أداة الدراسة:

تم اختبار الصدق والثبات من خلال تقييم نموذج القياس كما سيأتي.

الأساليب الإحصائية المستخدمة:

تم استخدام نمذجة المعادلة البنائية القائمة على المربعات الصغرى الجزئية (Partial Least Squares Structural Equation Modeling [PLS-SEM]) في تقييم نموذج القياس، وتقييم النموذج البنائي، واختبار الفرضيات.

نتائج الدراسة ومناقشتها:

تم تقييم نموذج الدراسة باستخدام برنامج المربعات الصغرى الجزئية (SmartPLS V.3.2.8) على مرحلتين: تقييم نموذج القياس، وعندما يحقق نموذج القياس المعايير المطلوبة، يتم تقييم النموذج البنائي، واختبار الفرضيات.

تقييم نموذج القياس:

يصف نموذج القياس علاقة الارتباط بين الأبعاد وفقراتها (Hair et al., 2017)، ويتم تقييم نموذج القياس من خلال الاختبارات الخاصة بالصدق والثبات؛ حيث يشير صدق المقياس إلى قدرته أداء المقياس على تحقيق الغرض الذي أنشئت من أجله، ويعبر صدق المقياس عن دقته، ويشير ثبات المقياس إلى قدرته على قياس المطلوب تحت عدد ظروف، ويعبر ثبات المقياس عن اتساقه.

تقييم نموذج القياس الانعكاسي لأبعاد الدرجة الأولى:

تكون العلاقة السببية من الأبعاد إلى الفقرات، ويجب أن يكون الارتباط بين فقرات البعد عالياً، ويمكن حذف بعض الفقرات من البعد دون أن تؤثر على البعد كليا (Hair et al., 2017; Hair et al., 2019).

الخطوة الأولى: تقييم ثبات المؤشر:

يتحقق ثبات المؤشر عندما يكون التشعب الخارجي لكل فقرة أعلى من (0.708)؛ ويعني هذا أن البعد يفسر أكثر من 50% من تباين فقراته (Hair et al., 2019)، وتشير النتائج إلى أن عدد الفقرات التي يجب حذفها 9 فقرات، وفقاً للآتي: (1) تم حذف الفقرات التي تشعبها أقل من (0.708)، وقد أدى حذفها إلى زيادة الثبات المركب ومتوسط التباين المفسر، وهي: مخاطر السلامة 42، ومخاطر التوافر 46، والمخاطر العامة 51، والضوابط التقنية 57، والضوابط التقنية 58، والضوابط التقنية 59، والضوابط التقنية 60، والضوابط التقنية 71، والضوابط الإدارية 75، (2) هناك فقرتان (مخاطر التوافر 44، والضوابط التقنية 64) تشعبهما أقل من (0.708)، ومع ذلك لم تُحذف؛ لأن حذفهما لا يؤدي إلى زيادة الثبات المركب أو متوسط التباين المفسر، وبعد ذلك يمكن القول: إن جميع الفقرات المتبقية تقيس الأبعاد بدرجة عالية من الثبات، ويوضح الجدول (2) التشعب الخارجي للفقرات المتبقية بعد الحذف.

جدول (2): تقييم نموذج القياس

المتغيرات	الأبعاد	الفقرات	التشبع Loadings	ألفا كرونباخ (α)	الثبات المركب (CR)	متوسط التباين المفسر (AVE)
الضوابط الأمنية	الضوابط التقنية	الضوابط_التقنية61	0.700	0.929	0.939	0.586
		الضوابط_التقنية62	0.725			
		الضوابط_التقنية63	0.700			
		الضوابط_التقنية64	0.838			
		الضوابط_التقنية65	0.820			
		الضوابط_التقنية66	0.797			
		الضوابط_التقنية67	0.819			
		الضوابط_التقنية68	0.806			
		الضوابط_التقنية69	0.774			
		الضوابط_التقنية70	0.706			
الضوابط الإدارية	الضوابط	الضوابط_التقنية72	0.717	0.944	0.952	0.642
		الضوابط_الإدارية73	0.744			
		الضوابط_الإدارية74	0.755			
		الضوابط_الإدارية76	0.845			
		الضوابط_الإدارية77	0.848			
		الضوابط_الإدارية78	0.800			
		الضوابط_الإدارية79	0.825			
		الضوابط_الإدارية80	0.755			
		الضوابط_الإدارية81	0.794			
		الضوابط_الإدارية82	0.822			
		الضوابط_الإدارية83	0.774			
		الضوابط_الإدارية84	0.840			

جدول (2): 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 السلامة	مخاطر السلامة	مخاطر السرية 36	0.821	0.868	0.905	0.655
		مخاطر السلامة 37	0.772			
		مخاطر السلامة 38	0.811			
		مخاطر السلامة 39	0.858			
		مخاطر السلامة 40	0.848			
		مخاطر السلامة 41	0.754			
		مخاطر التوافر 43	0.758	0.831	0.880	0.596
مخاطر التوافر	مخاطر التوافر	مخاطر التوافر 44	0.721			
		مخاطر التوافر 45	0.799			
		مخاطر التوافر 47	0.822			
		مخاطر التوافر 48	0.756			
		المخاطر العامة 49	0.795	0.923	0.938	0.684
	المخاطر العامة (المشتركة)	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:

تم استخدام الثبات المركب (CR) Composite Reliability في تقييم ثبات الاتساق الداخلي للأبعاد، وتتراوح قيمة الثبات المركب بين (0 و 1)؛ حيث تشير القيم العالية إلى درجات ثبات عالية، ويجب أن تكون قيمة الثبات المركب للبعد بين (0.70-0.95)، فإذا كانت أكبر من (0.95) فتعد مشكلة؛ أي أن الفقرات متشابهة، وتؤثر على مصداقية البيانات، وتؤدي إلى زيادة الخطأ، أيضاً يمكن استخدام معامل ألفا كرونباخ (α) كمقياس آخر لتقييم ثبات الاتساق الداخلي للأبعاد، وله نفس قيم الثبات المركب، إلا أنه ينتج عنه قيم أقل دقة من الثبات المركب (Hair et al., 2017).

وقد أظهرت النتائج في الجدول (2) أن قيم الثبات المركب للأبعاد تتراوح بين (0.880) و(0.952)، وقيم ألفا كرونباخ للأبعاد تتراوح بين (0.831) و(0.944)، وهذا يدل على أن جميع الأبعاد تتمتع بدرجة عالية من الثبات والاتساق الداخلي، وبالتالي فإن جميع الأبعاد تقيس الضوابط الأمنية والمخاطر بدرجة عالية من الثبات.

الخطوة الثالثة: تقييم صدق التقارب:

يجب أن يكون متوسط التباين المفسر (Average Variance Extracted [AVE]) للبعد (0.50) أو أكثر، لتوضح أن البعد يفسر 50% أو أكثر من التباين في فقراته، وإذا كانت أقل من (0.50)، فإن ذلك يشير إلى وجود تباين متبق؛ أي توجد أخطاء في الفقرات (Hair et al., 2017)، وتشير النتائج في الجدول (2) إلى أن قيم متوسط التباين المفسر لجميع الأبعاد تتراوح بين (0.586) و(0.684)، ويلاحظ أن هذه القيم تقع ضمن النطاق الموصى به، وهذا يدل على أن كل بُعد من الأبعاد يفسر أكثر من 50% من التباين في فقراته، وبالتالي يتحقق صدق تقارب الأبعاد.

الخطوة الرابعة: تقييم صدق التمايز:

صدق التمايز يعني أن البعد يتميز أو يختلف عن الأبعاد الأخرى، ويعكس ظواهر لا تمثلها الأبعاد الأخرى في النموذج (Hair et al., 2017)، ويمكن تقييم صدق التمايز من خلال الطرق الآتية:

(1) طريقة التشعبات المتقاطعة:

يجب أن يكون تشعبات الفقرات التابعة للبعد أكبر من تشعباتها المتقاطعة مع الأبعاد الأخرى (Hair et al., 2017)، وقد أظهرت النتائج في الجدول (3) أن تشعبات الفقرات التابعة لكل بُعد (القيم الغامقة) أعلى من تشعباتها المتقاطعة مع الأبعاد الأخرى، وتشير هذه النتيجة إلى عدم تداخل فقرات القياس فيما بينها؛ أي تتميز أو تختلف فقرات كل بُعد عن فقرات الأبعاد الأخرى.

جدول (3): تقييم صدق تمايز الفقرات باستخدام طريقة التشعبات المتقاطعة

الفقرات	الأبعاد	الضوابط الادارية	الضوابط التقنية	المخاطر العامة	مخاطر التوافر	مخاطر السلامة	مخاطر السرية
الضوابط الإدارية 73	0.744	0.573	-0.210	-0.238	-0.193	-0.290	
الضوابط الإدارية 74	0.755	0.556	-0.171	-0.246	-0.194	-0.280	
الضوابط الإدارية 76	0.845	0.613	-0.263	-0.315	-0.281	-0.310	
الضوابط الإدارية 77	0.848	0.611	-0.308	-0.359	-0.322	-0.347	
الضوابط الإدارية 78	0.800	0.626	-0.267	-0.278	-0.269	-0.269	
الضوابط الإدارية 79	0.825	0.559	-0.228	-0.269	-0.271	-0.251	
الضوابط الإدارية 80	0.755	0.431	-0.083	-0.208	-0.103	-0.165	
الضوابط الإدارية 81	0.794	0.450	-0.155	-0.253	-0.168	-0.237	
الضوابط الإدارية 82	0.822	0.492	-0.278	-0.351	-0.288	-0.342	
الضوابط الإدارية 83	0.774	0.457	-0.304	-0.364	-0.294	-0.325	
الضوابط الإدارية 84	0.840	0.607	-0.326	-0.356	-0.332	-0.343	
الضوابط التقنية 61	0.484	0.700	-0.322	-0.330	-0.303	-0.324	
الضوابط التقنية 62	0.496	0.725	-0.179	-0.191	-0.137	-0.207	
الضوابط التقنية 63	0.354	0.700	-0.212	-0.205	-0.157	-0.185	
الضوابط التقنية 64	0.504	0.838	-0.332	-0.327	-0.235	-0.307	
الضوابط التقنية 65	0.552	0.820	-0.316	-0.334	-0.235	-0.288	
الضوابط التقنية 66	0.506	0.797	-0.311	-0.339	-0.229	-0.279	
الضوابط التقنية 67	0.464	0.819	-0.275	-0.253	-0.220	-0.312	

جدول (3): يتبع

مخاطر السرية	مخاطر السلامة	مخاطر التوافر	المخاطر العامة	الضوابط التقنية	الضوابط الإدارية	الأبعاد الفقرات
-0.371	-0.278	-0.356	-0.410	0.806	0.558	الضوابط التقنية 68
-0.372	-0.325	-0.366	-0.395	0.774	0.625	الضوابط التقنية 69
-0.351	-0.245	-0.304	-0.311	0.706	0.537	الضوابط التقنية 70
-0.419	-0.339	-0.356	-0.388	0.717	0.624	الضوابط التقنية 72
0.628	0.548	0.565	0.795	-0.351	-0.254	المخاطر العامة 49
0.700	0.596	0.672	0.829	-0.314	-0.235	المخاطر العامة 50
0.548	0.531	0.565	0.785	-0.329	-0.208	المخاطر العامة 52
0.577	0.546	0.600	0.849	-0.357	-0.245	المخاطر العامة 53
0.648	0.618	0.670	0.899	-0.369	-0.276	المخاطر العامة 54
0.620	0.556	0.584	0.829	-0.341	-0.235	المخاطر العامة 55
0.568	0.531	0.628	0.798	-0.347	-0.272	المخاطر العامة 56
0.564	0.596	0.758	0.618	-0.316	-0.331	مخاطر التوافر 43
0.543	0.569	0.721	0.567	-0.289	-0.264	مخاطر التوافر 44
0.632	0.534	0.799	0.591	-0.365	-0.318	مخاطر التوافر 45
0.556	0.545	0.822	0.586	-0.305	-0.259	مخاطر التوافر 47
0.470	0.483	0.756	0.467	-0.263	-0.234	مخاطر التوافر 48
0.520	0.772	0.521	0.522	-0.217	-0.270	مخاطر السلامة 37
0.546	0.811	0.573	0.580	-0.283	-0.229	مخاطر السلامة 38
0.590	0.858	0.580	0.544	-0.291	-0.267	مخاطر السلامة 39
0.593	0.848	0.612	0.558	-0.290	-0.290	مخاطر السلامة 40
0.542	0.754	0.600	0.549	-0.241	-0.207	مخاطر السلامة 41
0.762	0.443	0.542	0.496	-0.279	-0.314	مخاطر السرية 29
0.836	0.528	0.596	0.573	-0.345	-0.364	مخاطر السرية 30
0.858	0.619	0.617	0.625	-0.361	-0.336	مخاطر السرية 31
0.793	0.570	0.559	0.627	-0.349	-0.303	مخاطر السرية 32
0.785	0.534	0.578	0.597	-0.341	-0.243	مخاطر السرية 33
0.815	0.573	0.542	0.583	-0.341	-0.260	مخاطر السرية 34
0.794	0.564	0.620	0.638	-0.330	-0.253	مخاطر السرية 35
0.821	0.624	0.636	0.665	-0.318	-0.258	مخاطر السرية 36

2) طريقة نسبة أحادية وتغاير السمة :

ينبغي أن تكون قيم نسبة أحادية وتغاير السمة (Heterotrait-monotrait Ratio) (HTMT) أقل من (0.85)، والتي تدل على عدم وجود ارتباط عالٍ بين البُعد وبقية الأبعاد الأخرى، وأن البُعد يختلف عن بقية الأبعاد الأخرى (Henseler et al., 2015)، وقد أظهرت النتائج في الجدول (4) أن جميع قيم نسبة أحادية وتغاير السمة تتراوح بين (0.314) و(0.835)، (ويلاحظ أن هذه القيم أقل من 0.85)، وتشير هذه النتيجة إلى صدق تمايز الأبعاد، وعدم وجود ارتباط عالٍ بين البُعد وبقية الأبعاد الأخرى، وأن البُعد يختلف عن بقية الأبعاد الأخرى.

جدول (4): تقييم صدق تمايز الأبعاد باستخدام طريقة نسبة أحادية وتغاير السمة (HTMT)

الأبعاد	الضوابط الادارية	الضوابط التقنية	المخاطر العامة	مخاطر التوافر	مخاطر السلامة	مخاطر السرية
الضوابط الادارية						
الضوابط التقنية	0.719					
المخاطر العامة	0.314	0.443				
مخاطر التوافر	0.409	0.449	0.835			
مخاطر السلامة	0.340	0.358	0.760	0.833		
مخاطر السرية	0.383	0.437	0.803	0.817	0.769	

تقييم نموذج القياس الانعكاسي لأبعاد الدرجة الثانية :

اعتمدت الدراسة الحالية في تقييم نموذج القياس الانعكاسي لأبعاد الدرجة الثانية على طريقة المرحلتين المنفصلة؛ حيث يتم قياس أبعاد الدرجة الأولى في المرحلة الأولى بدون قياس أبعاد الدرجة الثانية، ثم يتم استخدام المتوسطات المعيارية لأبعاد الدرجة الأولى كمؤشرات لأبعاد الدرجة الثانية في المرحلة الثانية، وقد أظهرت نتائج التقييم الآتي:

(1) ثبات المؤشر (الأبعاد من الدرجة الأولى): يظهر في الجدول (5) أن تشبع جميع مؤشرات المتغيرات أكبر من (0.708)؛ وهذا يدل على أن أبعاد الدرجة الأولى (المؤشرات) تتمتع بثبات عالٍ.

(2) ثبات الاتساق الداخلي (الأبعاد من الدرجة الثانية): يظهر في الجدول (5) أن جميع قيم الثبات المركب وألفا كرونباخ تقع بين (0.70-0.95)؛ وهذا يدل على أن الاتساق الداخلي لأبعاد الدرجة الثانية تتمتع بثبات عالٍ.

(3) صدق التقارب (الأبعاد من الدرجة الثانية): يظهر في الجدول (5) أن جميع قيم متوسط التباين المفسر أكبر من (0.50)؛ وهذا يدل على أن أبعاد الدرجة الثانية تفسر أكثر من 50% من التباين في أبعادها.

جدول (5): تقييم ثبات المؤشر، والاتساق الداخلي، وصدق التقارب

الأبعاد من الدرجة الثانية (المتغيرات)	الأبعاد من الدرجة الأولى (المؤشرات)	التشبع	ثبات المؤشر	ألفا كرونباخ (α)	الثبات المركب (CR)	متوسط التباين المفسر (AVE)
مخاطر تكنولوجيا المعلومات	مخاطر السرية	0.897	0.805	0.909	0.936	0.785
	مخاطر السلامة	0.861	0.741			
	مخاطر التوافر	0.895	0.801			
	المخاطر العامة	0.891	0.794			
الضوابط الأمنية	الضوابط التقنية	0.922	0.850	0.810	0.913	0.840
	الضوابط الإدارية	0.911	0.830			

4) صدق التمايز (الأبعاد من الدرجة الثانية):

يظهر في الجدول (6) أن قيم نسبة أحادية وتغاير السمة (HTMT) أقل من (0.85)؛ وهذا يدل على صدق تمايز الأبعاد من الدرجة الثانية، وعدم وجود ارتباط عال بين البُعد من الدرجة الثانية وبقيّة الأبعاد الأخرى، وأن البُعد من الدرجة الثانية يختلف عن بقيّة الأبعاد الأخرى.

جدول (6): تقييم صدق تمايز أبعاد الدرجة الثانية باستخدام طريقة (HTMT)

المتغيرات	الضوابط الأمنية	مخاطر تكنولوجيا المعلومات
الضوابط الأمنية		
مخاطر تكنولوجيا المعلومات	0.516	

تقييم النموذج البنائي للمتغيرات الكلية من الدرجة الثانية:

أكدت نتائج تقييم نموذج القياس الانعكاسي أن المقاييس تتسم بالصدق والثبات، وفي هذه المرحلة سيتم تقييم النموذج البنائي (النموذج الداخلي Inner model) لاختبار مستوى الترابط والعلاقة فيما بين المتغيرات باستخدام نمذجة المعادلة البنائية القائمة على المربعات الصغرى الجزئية (PLS-SEM).

أولاً: تقييم الارتباط الخطي المشترك:

تم فحص الارتباط الخطي المشترك بين أبعاد مخاطر تكنولوجيا المعلومات باستخدام معامل تضخم التباين (Variance Inflation Factor – VIF)، إلى جانب مؤشر التباين المسموح به (Tolerance Index – TI)، للتحقق من عدم وجود مشكلة جوهرية في الارتباط الخطي المشترك بين المتغيرات المفردة. وتشير القيم المنخفضة لمعامل (VIF) وارتفاع قيم (TI) إلى انخفاض احتمال وجود مشكلة الارتباط الخطي المشترك. ويُستدل على عدم وجود مشكلة جوهرية عندما تكون قيم (VIF) أقل من (5) وقيم (TI) أكبر من (0.20). ويوضح جدول (7) نتائج اختبار الارتباط الخطي المشترك على مستوى أبعاد مخاطر تكنولوجيا المعلومات.

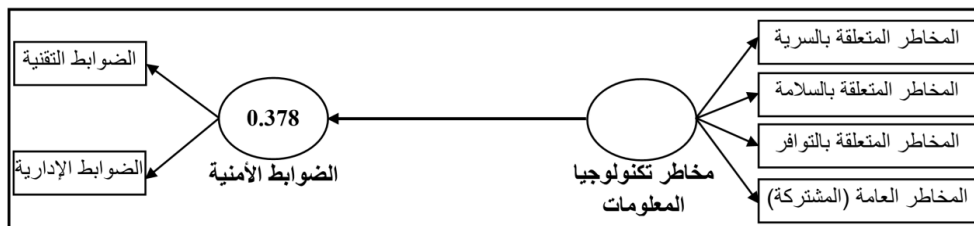
جدول (7): نتائج اختبار الارتباط الخطي المشترك بين أبعاد مخاطر تكنولوجيا المعلومات

أبعاد مخاطر تكنولوجيا المعلومات	التباين المسموح به (TI)	معامل تضخم التباين (VIF)
مخاطر السرية	0.375	2.670
مخاطر السلامة	0.411	2.433
مخاطر التوافر	0.382	2.620
المخاطر العامة	0.373	2.678

يتضح من الجدول (7) أن قيم معامل تضخم التباين (VIF) لأبعاد مخاطر تكنولوجيا المعلومات تراوحت بين (2.433–2.678)، في حين تراوحت قيم التباين المسموح به (TI) بين (0.373–0.411). وبذلك جاءت جميع قيم (VIF) أقل من (5)، وجميع قيم (TI) أكبر من (0.20)، مما يشير إلى عدم وجود مشكلة جوهرية في الارتباط الخطي المشترك بين أبعاد مخاطر تكنولوجيا المعلومات.

ثانياً: معامل التحديد:

إن معامل التحديد يُفسر التباين الكلي في المتغيرات الكامنة الداخلية (قدرة المتغيرات المستقلة على تفسير التباين في المتغير التابع)، ومعامل التحديد هو مقياس للقوة التفسيرية للنموذج، وتتراوح قيمة معامل التحديد (R^2) بين (0 و1)؛ حيث تشير القيم العليا إلى مستويات أعلى في القوة التفسيرية، ويتم تحديد قدرة النموذج البحثي على تفسير المتغير التابع من خلال قيمة معامل التحديد (R^2) التي تقدر بـ (0.67) أو (0.33) أو (0.19) قوية، أو متوسطة، أو ضعيفة على التوالي وفقاً لـ Chin (1998). ويوضح الشكل (3) نتائج تقييم معامل التحديد.



شكل (3): تقييم معامل التحديد

وقد أظهرت النتائج في الشكل (3) أن قيمة معامل التحديد للضوابط الأمنية هي: (0.378)؛ وهذا يشير إلى أن مخاطر تكنولوجيا المعلومات تفسر ما نسبته 37.8% من التباين في الضوابط الأمنية، وهي نسبة متوسطة؛ كونها أكبر من (0.33)، وأقل من (0.67)، وبالتالي فإن القوة التفسيرية للنموذج متوسطة.

ثالثاً: ملائمة التنبؤ:

يكون للنموذج أهمية تنبؤية عندما تكون قيمة ملائمة التنبؤ (Q^2) أكبر من الصفر، وكلما زادت قيمة ملائمة التنبؤ (Q^2) زادت أهمية النموذج من حيث التنبؤ، وإذا كانت مساوية للصفر فيعد ذلك مؤشراً على أن النموذج ليس لديه دقة تنبؤية، وغير ملائم من حيث التنبؤ. وقيم ملائمة التنبؤ (Q^2) أعلى من (0) أو (0.25) أو (0.50) والتي تشير إلى أن الملائمة التنبؤية منخفضة أو متوسطة أو عالية لنموذج مسار PLS على التوالي (Hair et al., 2019). والجدول (8) يُبين نتائج تقييم ملائمة النموذج للتنبؤ.

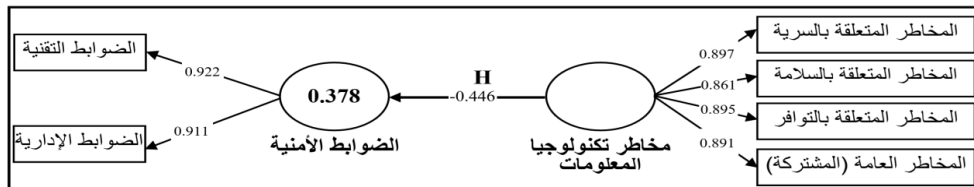
جدول (8): تقييم ملائمة التنبؤ

المتغيرات	(SSO) مجموع مربع المشاهدات	(SSE) مجموع مربع أخطاء التنبؤ	$Q^2 (= 1 - SSE/SSO)$	التقدير
الضوابط الأمنية	436	367.739	0.157	منخفضة

يتضح من الجدول (8) أن قيمة ملائمة التنبؤ (Q^2) للضوابط الأمنية تساوي (0.157)، وهي نسبة مقبولة، ولكنها منخفضة، وبالتالي يمكن القول: إن للنموذج أهمية تنبؤية؛ كون قيمة ملائمة التنبؤ (Q^2) أكبر من الصفر.

رابعاً: تقييم معاملات المسار:

إن قيم معاملات المسار تقع ضمن نطاق (1)، وتمثل القيم القريبة من (+1) علاقة 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 بدرجة واحدة ينشأ عنها تغيير في المتغير التابع بقدر حجم معامل المسار على فرض ثبات جميع المتغيرات الأخرى ومعاملات مساراتها، وقد تم إجراء Bootstrapping باستخدام برنامج المربعات الصغرى الجزئية (PLS) لاختبار الفرضيات المقترحة بين متغيرات الدراسة الحالية، ويوضح الشكل (4) نتائج تقييم معاملات المسار.



شكل (4): تقييم معاملات المسار على مستوى المتغيرات

اختبار فرضيات الدراسة :

اختبار الفرضية الرئيسية :

H: تؤثر مخاطر تكنولوجيا المعلومات سلباً في الضوابط الأمنية لدى شركات الاتصالات مجتمع الدراسة، ويظهر في الجدول (9) نتائج اختبار الفرضية الرئيسية.

جدول (9): اختبار الفرضية الرئيسية

المسار	معامل المسار β	الانحراف المعياري	إحصائية t	الدلالة p
مخاطر تكنولوجيا المعلومات -> الضوابط الأمنية	-0.446	0.060	7.480	0.000

أظهرت النتائج في الجدول (9) أن مخاطر تكنولوجيا المعلومات تؤثر سلباً في الضوابط الأمنية لدى شركات الاتصالات في صنعاء؛ حيث كانت قيمة معامل المسار ($\beta = -0.446$)، وقيمة ($t = 7.480$) دالة إحصائياً عند مستوى دلالة أقل من (0.01). وهذا يعني أن التغيير (الزيادة) في مخاطر تكنولوجيا المعلومات بدرجة واحدة ينشأ عنها تغيير (انخفاض) في الضوابط الأمنية بنسبة 44.6%، وبالتالي تدعم هذه النتيجة الفرضية الرئيسية.

وهذه النتيجة تتفق مع نظرية أمن المعلومات (Horne et al., 2016) التي تشير إلى أن العلاقة بين المخاطر والضوابط سلبية، فبعض المعلومات محمية من المخاطر من خلال الضوابط الأمنية لإنتاج مورد يمكن الاعتماد عليه. وأيضاً تتفق مع نظرية الردع العام (Straub & Welke, 1998) التي تفترض أن الإجراءات العامة تقلل من المخاطر بشكل مباشر أو غير مباشر من خلال استخدام الضوابط الأمنية، وكذلك تتفق مع دراسة Schuessler (2009) التي توصلت إلى أن المخاطر تؤثر في التدابير المضادة، فكلما زادت المخاطر التي تواجهها أنظمة الشركة يتم تنفيذ كل نوع من أنواع التدابير المضادة، كما أن تطبيق التدابير المضادة يغير طبيعة المخاطر التي تواجه المعلومات، وتتفق مع دراسة Al-ghananeem (2014) التي أكدت أن المخاطر لها تأثير سلبي في ضمان أمن المعلومات، وتتفق مع دراسة Straub (1987) التي أظهرت أن العلاقة السببية قوية بين جهود الردع وانخفاض الضرر، وأن الوقاية أداة فاعلة في الحد من إساءة الاستخدام، غير أن دراسة Riad (2009) أشارت إلى عدم وجود فجوة بين المخاطر والضوابط في الشركات البريطانية.

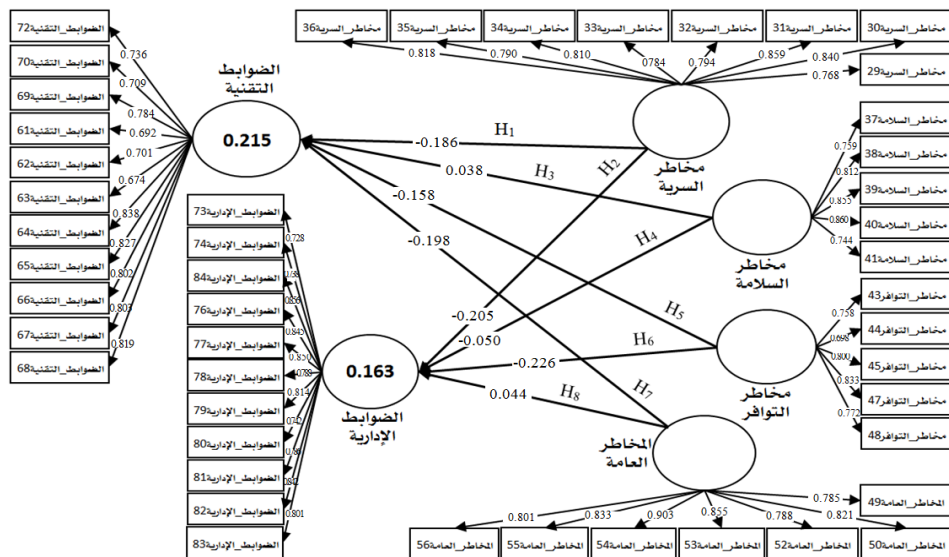
وتؤكد نتيجة الدراسة الحالية والنظريات والدراسات السابقة أن المخاطر تؤثر سلباً في الضوابط الأمنية، ويرجع ذلك إلى الثغرات الأمنية التي تنشأ مع مرور الزمن الناتجة عن عوامل تنظيمية وتكنولوجية تؤدي إلى ظهور مخاطر جديدة، وتصبح الضوابط الأمنية الحالية غير كافية؛ حيث يستغل المهاجمون الثغرات الأمنية في الأنظمة، أو الشبكات، أو خطط الطوارئ، أو آليات المصادقة والتشفير، أو قصور في الجوانب التشريعية والتنظيمية المتعلقة بحماية المعلومات، أو قصور في تحديث أنظمة الحماية، أو قصور في تنفيذ برامج التوعية والتدريب، أو قصور في تنفيذ ومراجعة وتحديث سياسة الأمن، وهذه الثغرات تمكن المهاجمين من تجاوز الضوابط الأمنية، والوصول إلى المعلومات وكشفها، أو تعديلها، أو حذفها، وإحداث الضرر، وبالتالي تؤثر المخاطر في الضوابط، ومن جانب آخر، يُمكن القول: إن الضوابط الأمنية تحد من المخاطر وبدرجات متفاوتة، ومقدار المخاطر التي يمكن خفضها تعتمد بشكل كبير على إدراك النطاق الكامل للضوابط الأمنية الملائمة، وتنفيذ أكثرها فاعلية وتحديثها، فنجد شركات مخاطرها منخفضة أو متوسطة، وأخرى مرتفعة، فاستخدام الضوابط الأمنية الملائمة يخفف المخاطر.

اختبار الفرضيات الفرعية للفرضية الرئيسية :

ويتفرع من الفرضية الرئيسية ثمان فرضيات فرعية، تتمثل بالآتي:

- H1: تؤثر المخاطر المتعلقة بالسرية سلباً في الضوابط التقنية لدى شركات الاتصالات في صنعاء.
- H2: تؤثر المخاطر المتعلقة بالسرية سلباً في الضوابط الإدارية لدى شركات الاتصالات في صنعاء.
- H3: تؤثر المخاطر المتعلقة بالسلامة سلباً في الضوابط التقنية لدى شركات الاتصالات في صنعاء.
- H4: تؤثر المخاطر المتعلقة بالسلامة سلباً في الضوابط الإدارية لدى شركات الاتصالات في صنعاء.

- H5: تؤثر المخاطر المتعلقة بالتوافر سلباً في الضوابط التقنية لدى شركات الاتصالات في صناعة.
H6: تؤثر المخاطر المتعلقة بالتوافر سلباً في الضوابط الإدارية لدى شركات الاتصالات في صناعة.
H7: تؤثر المخاطر العامة سلباً في الضوابط التقنية لدى شركات الاتصالات في صناعة.
H8: تؤثر المخاطر العامة سلباً في الضوابط الإدارية لدى شركات الاتصالات في صناعة.
ويوضح الشكل (5) نتائج تقييم معاملات المسار على مستوى الأبعاد.



شكل (5): تقييم معاملات المسار على مستوى الأبعاد

يظهر في الشكل (5) أن قيمة معامل التحديد (R^2) لبُعد الضوابط التقنية (0.215)؛ وهذا يشير إلى أن مخاطر السرية، ومخاطر السلامة، ومخاطر التوافر، والمخاطر العامة تُفسر ما نسبته 21.5% من التباين في الضوابط التقنية، وقيمة معامل التحديد (R^2) لبُعد الضوابط الإدارية هو (0.163)، وهذا يشير إلى أن مخاطر السرية، ومخاطر السلامة، ومخاطر التوافر، والمخاطر العامة تُفسر ما نسبته 16.3% من التباين في الضوابط الإدارية. وبين الشكل (5) قيم معاملات المسار، ويوضح الجدول (10) نتائج اختبار الفرضيات الفرعية.

جدول (10): اختبار الفرضيات الفرعية للفرضية الرئيسية

م	المسار	معامل المسار β	الانحراف المعياري	إحصائية t	مستوى الدلالة p
1	مخاطر السرية - < الضوابط التقنية	-0.186	0.099	1.969	0.030
2	مخاطر السرية - < الضوابط الإدارية	-0.205	0.107	1.974	0.028
3	مخاطر السلامة - < الضوابط التقنية	0.038	0.095	0.402	0.344
4	مخاطر السلامة - < الضوابط الإدارية	-0.050	0.094	0.526	0.299
5	مخاطر التوافر - < الضوابط التقنية	-0.158	0.095	1.967	0.048
6	مخاطر التوافر - < الضوابط الإدارية	-0.226	0.106	2.139	0.016
7	المخاطر العامة - < الضوابط التقنية	-0.198	0.122	1.981	0.043
8	المخاطر العامة - < الضوابط الإدارية	0.044	0.117	0.377	0.353

الفرضية الفرعية الأولى:

أظهرت النتائج في الجدول (10) أن مخاطر السرية تؤثر سلباً في الضوابط التقنية لدى شركات الاتصالات في صنعاء؛ حيث كانت قيمة معامل المسار ($\beta = -0.186$)، وقيمة ($t = 1.969$) دالة إحصائياً عند مستوى دلالة أقل من (0.05)؛ وهذا يعني أن التغيير (بالزيادة) في مخاطر السرية بدرجة واحدة ينشأ عنها تغيير (انخفاض) في الضوابط التقنية بنسبة 18.6%، وهذه النتيجة تدعم صحة الفرضية الفرعية الأولى.

وتتفق هذه النتيجة مع دراسة Schuessler (2009) التي توصلت إلى أن المخاطر (الهندسة الاجتماعية، والتجسس، والأفعال المتعمدة) تؤثر في التدابير الوقائية (استغلال الثغرات في التدابير الوقائية) المتمثلة في استخدام الجدران النارية، وأنظمة منع التسلسل، وبرامج الحماية من الفيروسات. وتتفق مع دراسة Atyam (2010) التي أشارت إلى أن الوصول غير المصرح به للبيانات يؤثر بشكل كبير في أنظمة الشركات، وهو ناجم عن ضعف آليات التحقق من الهوية. وتتفق مع دراسة Ahmed et al. (2017) التي ذكرت أن الوصول غير المصرح به إلى المعلومات السرية ناجم عن عدم كفاية إجراءات المصادقة، ومن جانب آخر وجدت الدراسة أن التشفير والتوقيع الرقمي يحدان من هجمات التنصت، وأيضاً أكدت دراسة Azees et al. (2016) أن التدابير المضادة (تقنيات التشفير، والمصادقة القوية، والتوقيع الرقمي) تقلل من مخاطر التنصت والابتزاز.

ويلاحظ أن مخاطر السرية كالتنصت، والوصول غير المصرح به، والاصطياد الإلكتروني لها ارتباط عالٍ عكسي مع الضوابط التقنية كالتحكم بالوصول، والمصادقة، ومكافح البرامج الضارة، فكلما زادت المخاطر المتعلقة بالسرية انخفض مستوى الضوابط التقنية، وكلما زاد مستوى الضوابط التقنية انخفضت المخاطر المتعلقة بالسرية، وغالباً ما تستغل مخاطر السرية نقاط الضعف في الضوابط التقنية (ثغرات في النظام، أو الشبكة، أو الضوابط الأمنية) التي تمكن المهاجمين من الوصول إلى أنظمة المعلومات، والحصول على المعلومات الحساسة، وفتح ثغرات (أبواب خلفية) في النظام تمكن المهاجم من الوصول إلى أنظمة المعلومات لاحقاً.

الفرضية الفرعية الثانية:

أشارت النتائج في الجدول (10) إلى أن مخاطر السرية تؤثر سلباً في الضوابط الإدارية لدى شركات الاتصالات في صنعاء؛ حيث كانت قيمة معامل المسار ($\beta = -0.205$)، وقيمة ($t = 1.974$) دالة إحصائياً عند مستوى دلالة أقل من (0.05)؛ وهذا يعني أن التغيير (بالزيادة) في مخاطر السرية بدرجة واحدة ينشأ عنها تغيير (انخفاض) في الضوابط الإدارية بنسبة 20.5%، وهذه النتيجة تدعم صحة الفرضية الفرعية الثانية للفرضية الرئيسية.

وتتفق هذه النتيجة مع دراسة Schuessler (2009) التي توصلت إلى أن الوصول غير المصرح به، وعدم الامتثال للسياسات، والأفعال المتعمدة المتعلقة بالسرقة والابتزاز تؤثر في التدابير المضادة (الردع) المتمثلة في برامج التوعية والتدريب، واختبار الاختراق/ إجراءات التدقيق، وتنفيذ السياسة الأمنية. وتتفق مع دراسة Atyam (2010) التي أظهرت أن الوصول غير المصرح به من قبل المستخدمين له تأثير مرتفع على منظمات الأعمال، وهو ناجم عن ضعف إدارة كلمات المرور، وعدم مراجعة مستويات وصول المستخدم إلى النظام. وتتفق مع دراسة Ahmed et al. (2017) التي ذكرت أن حدوث هجمات التنصت وكسر كلمة المرور (بغرض الحصول على المعلومات السرية) ناجم عن ضعف برامج التوعية والتدريب وعدم التشفير، ومن جانب آخر وجدت الدراسة أن برامج التوعية والتدريب وعدم الكشف عن الهوية تحد من هجمات الهندسة الاجتماعية والاصطياد الإلكتروني.

ويلاحظ أن مخاطر السرية تؤثر سلباً في الضوابط الإدارية، وقد يرجع ذلك إلى ضعف برامج التوعية والتدريب، أو وجود ثغرات في السياسة الأمنية، أو قصور في خطط الطوارئ، أو قصور في الجوانب

التشريعية والتنظيمية المتعلقة بأمن المعلومات، وقد يستغل المهاجمون (الهندسة الاجتماعية، والاصطياد الإلكتروني، وكسر كلمة المرور) سلوك المستخدمين؛ للوصول إلى كلمة المرور، والحصول على المعلومات الحساسة، ويُعد العنصر البشري الحلقة الأضعف في أمن المعلومات؛ بسبب الإهمال أو اللامبالاة، وقد يتسبب المستخدمون في حدوث الكثير من الهجمات الناتجة عن ضعف كلمة المرور، والتحكم غير الملائم بالأجهزة، والإخفاق في تحديث أنظمة الحماية، وتصفح مواقع ويب المصابة بالبرامج الضارة، والاستجابة لرسائل البريد الإلكتروني الخادعة وغيرها.

الفرضية الفرعية الثالثة:

أظهرت النتائج في الجدول (10) أن مخاطر السلامة لها تأثير غير دال في الضوابط التقنية لدى شركات الاتصالات في صنعاء؛ حيث كانت قيمة معامل المسار ($\beta=0.038$)، وقيمة ($t=0.402$) غير دالة إحصائياً عند مستوى دلالة أقل من (0.05)، وهذه النتيجة لا تدعم صحة الفرضية الفرعية الثالثة.

وتختلف هذه النتيجة مع دراسة Schuessler (2009) التي توصلت إلى أن أفعال الموظفين المتعمد وغير المتعمد، وأخطاء البرمجيات الفنية تؤثر في التدابير المضادة (تدابير الكشف) المتمثلة في التحكم بالوصول المادي، وأنظمة الإنذار، والشبكات الخاصة الافتراضية، ومن جانب آخر، وجدت دراسة Straub (1987) أن التدابير الوقائية تحد من إساءة استخدام الحاسوب، وأن المخاطر تدفع المنظمات إلى استخدام التدابير المضادة الملائمة، وأشارت دراسة Azees et al. (2016) إلى أن التدابير المضادة (التوقيع الرقمي، وتشفير البيانات الحساسة) تحد من هجمات تعديل البيانات.

وقد يرجع اختلاف نتيجة الدراسة الحالية عن الدراسات السابقة إلى اختلاف القطاع أو البيئة التي أجريت فيها الدراسة؛ كون الدراسات أجريت في قطاعات وبيئات مختلفة، أو انخفاض المخاطر المتعلقة بتعديل أو إتلاف البيانات المتعمد وغير المتعمد، وانخفاض أخطاء البرمجيات الفنية والتقدم التكنولوجي في قطاع الاتصالات؛ نظراً لفاعلية إجراءات الحماية واستخدام الضوابط التقنية الملائمة، أو أن هناك تحيزاً في الاستجابة من قبل الموظفين؛ كون أغلب فقرات بُعد مخاطر السلامة تتعلق بالإدخال والإتلاف المتعمد وغير المتعمد من قبل الموظفين، وباعتقادي أن السبب الأخير هو الأقرب للدقة، ويؤيد هذا التفسير اعتدال بعض الموظفين في قطاع الاتصالات عن تقديم المعلومات اللازمة بحجة سرية المعلومات.

الفرضية الفرعية الرابعة:

أشارت النتائج في الجدول (10) إلى أن مخاطر السلامة لها تأثير غير دال إحصائياً في الضوابط الإدارية لدى شركات الاتصالات في صنعاء؛ حيث كانت قيمة معامل المسار ($\beta=-0.050$)، وقيمة ($t=0.526$) غير دالة عند مستوى دلالة أقل من (0.05)، وهذه النتيجة لا تدعم صحة الفرضية الفرعية الرابعة.

وتختلف هذه النتيجة مع دراسة Schuessler (2009) التي توصلت إلى أن الإتلاف والإدخال المتعمد وغير المتعمد للبيانات، وإخفاق أو أخطاء المستخدمين، وأخطاء البرمجيات الفنية تؤثر في تدابير الردع المتمثلة في الامتثال للقوانين واللوائح المتعلقة بحماية البيانات، والنسخ الاحتياطي، وبرامج التوعية والتدريب، وتختلف مع دراسة Atyam (2010) التي أظهرت أن الوصول والتعديل غير المصرح به له تأثير مرتفع على منظمات الأعمال والناجم عن ضعف الفصل بين الواجبات، ومن جانب آخر، وجدت دراسة Azees et al. (2016) أن التدابير المضادة (السياسة الأمنية المتعلقة بكلمة المرور) تحد من الهجمات التي تستهدف تعديل البيانات. وذكرت دراسة Jadrić et al. (2016) أن النسخ الاحتياطية تحد من مخاطر الأفعال المتعمد وغير المتعمد.

ويلاحظ أن نتيجة الدراسة الحالية تختلف عن الدراسات السابقة، وقد يرجع ذلك إلى انخفاض مخاطر السلامة في شركات الاتصالات؛ نظراً لفاعلية الضوابط الإدارية، أو قد يعود إلى ارتفاع مستوى الوعي والإدراك في مجال أمن المعلومات، وتطبيق السياسة الأمنية وتحديثها باستمرار، والامتثال للقوانين واللوائح المتعلقة بحماية البيانات، أو أن هناك تحيزاً في الاستجابة من قبل الموظفين؛ كون أغلب فقرات

هذا البُعد تتعلق بالإدخال والإتلاف المتعمد وغير المتعمد من قبل الموظفين، أو اختلاف البيئة أو القطاع؛ كون الدراسة أجريت في بيئات وقطاعات مختلفة.

ويلاحظ أن أغلب فقرات بُعد مخاطر السلامة تتضمن الإدخال والإتلاف المتعمد وغير المتعمد من قبل الموظفين، وقد تم رفض الفرضيات ذات الصلة بهذا البُعد، وهذا يؤكد صحة ما سبق تفسيره بأن هناك تحيزاً في الاستجابة من قبل الموظفين بحجة سرية المعلومات وحساسيتها.

الفرضية الفرعية الخامسة:

أكدت النتائج في الجدول (10) أن مخاطر التوافر تؤثر سلباً في الضوابط التقنية لدى شركات الاتصالات في صنعاء؛ حيث كانت قيمة معامل المسار ($\beta = -0.158$)، وقيمة ($t = 1.967$) دالة إحصائياً عند مستوى دلالة أقل من (0.05)؛ وهذا يعني أن التغيير (بالزيادة) في مخاطر التوافر بدرجة واحدة ينشأ عنها تغيير (انخفاض) في الضوابط التقنية بنسبة 15.8%، وهذه النتيجة تدعم صحة الفرضية الفرعية الخامسة.

وتتفق هذه النتيجة مع دراسة Schuessler (2009) التي وجدت أن الكوارث الطبيعية وأعطال الأجهزة الفنية تؤثر في التدابير الوقائية المتمثلة في الجدران النارية، وأنظمة منع التسلل، وإجراءات التصحيح والتحديث، والأمن المادي، ومن جانب آخر، أشارت دراسة Kumar et al. (2008) إلى أن الجدران النارية وأنظمة كشف التسلل تخفف من الآثار السلبية لهجمات الحرمان من الخدمة، وأيضاً، أظهرت دراسة Azees et al. (2016) أن التدابير المضادة (آليات المصادقة وأنظمة كشف التسلل) تحد من هجمات الحرمان من الخدمة.

وقد يرجع هذا الأثر السلبي إلى استغلال الثغرات في الضوابط التقنية (الثغرات في الشبكة أو البرامج أو النظام)، أو أن شركات الاتصالات أكثر عرضة لهذا النوع من المخاطر (هجمات الحرمان من الخدمة، والكوارث السياسية)، ويؤيد هذا التفسير تقرير Kaspersky (2016) الذي أشار إلى أن هجمات الحرمان من الخدمة لا تزال تشكل تهديداً خطيراً على مزودي خدمات الاتصالات في جميع أنحاء العالم، وقد تضررت شركات الاتصالات بهذه الهجمات أكثر من أي قطاع آخر، وأيضاً أكدت دراسة Whitman (2004) أن مزودي خدمات الاتصالات الأكثر تأثراً بتوافر الخدمة، وذكر تقرير المؤسسة العامة للاتصالات (الشوكان، 2016) أن الغياب الكامل للطاقة العمومية واختفاء المشتقات النفطية والحروب أثر على الأنشطة المختلفة لشركات الاتصالات.

الفرضية الفرعية السادسة:

أظهرت النتائج في الجدول (10) أن مخاطر التوافر تؤثر سلباً في الضوابط الإدارية لدى شركات الاتصالات في صنعاء؛ حيث كانت قيمة معامل المسار ($\beta = -0.226$)، وقيمة ($t = 2.139$) دالة إحصائياً عند مستوى دلالة أقل من (0.05)؛ وهذا يعني أن التغيير (بالزيادة) في مخاطر التوافر بدرجة واحدة ينشأ عنها تغيير (انخفاض) في الضوابط الإدارية بنسبة 22.6%، وهذه النتيجة تدعم صحة الفرضية الفرعية السادسة.

وتتفق هذه النتيجة مع دراسة Schuessler (2009) التي توصلت إلى أن المخاطر (هجمات الحرمان من الخدمة) تؤثر في تدابير الردع المتمثل في إجراءات التدقيق، والامتثال للقوانين واللوائح، ومن جانب آخر، ذكرت دراسة Banja (2012) أن النسخ الاحتياطي للبرامج والمعلومات يخفف مستوى المخاطر المتعلقة بالكوارث الطبيعية والسياسية. أيضاً أشارت دراسة Jadrić et al. (2016) إلى أن النسخ الاحتياطي يحد من مخاطر الكوارث الطبيعية وانقطاع الطاقة.

ويتضح أن مخاطر التوافر تؤثر سلباً في الضوابط الإدارية، وقد يعود هذا الأثر إلى استغلال الثغرات في الضوابط الإدارية، ومنها: ثغرات في خطة استمرارية العمل، أو ثغرات في خطة التعافي من الكوارث، أو قصور في النسخ الاحتياطي التي قد تؤدي إلى توقف النظام عن العمل، وكذلك يؤدي انقطاع الطاقة إلى

تدهور أداء الأنظمة وشبكات المعلومات والتخزين والمعالجة، وقد يتوقف النظام بشكل كلي، وباعتقادي أن التفسير الدقيق هو معاناة شركات الاتصالات في صنعاء من مشاكل الطاقة (غياب كلي للطاقة العمومية والاعتماد على المولدات والبطاريات) والكوارث السياسية (تضرر قطاع الاتصالات بشكل كبير والناجم عن الحروب)، وقد أدت هذه الكوارث إلى تعطل النظام، وتوقف الأعمال، وخسائر مالية، وإحاق أضرار بالسمعة، وفقدان الثقة.

الفرضية الفرعية السابعة:

أشارت النتائج في الجدول (10) إلى أن المخاطر العامة تؤثر سلباً في الضوابط التقنية لدى شركات الاتصالات في صنعاء؛ حيث كانت قيمة معامل المسار ($\beta = -0.198$)، وقيمة ($t = 1.981$) دالة إحصائياً عند مستوى دلالة أقل من (0.05)، وهذا يعني أن التغيير (بالزيادة) في المخاطر العامة بدرجة واحدة ينشأ عنها تغيير (انخفاض) في الضوابط التقنية بنسبة 19.8%، وهذه النتيجة تدعم صحة الفرضية الفرعية السابعة.

وتتفق هذه النتيجة مع دراسة Schuessler (2009) التي وجدت أن هجمات البرامج المتعمدة تؤثر في التدابير الوقائية المتمثلة في أنظمة منع التسلسل والجدران النارية وبرامج الحماية من الفيروسات، ومن جانب آخر، توصلت دراسة Straub (1990) إلى أن الجهود الوقائية تخفف حوادث إساءة الاستخدام، وأشارت دراسة Kumar et al. (2008) إلى أن مكافح الفيروسات يحد من الآثار السلبية للفيروسات، وذكرت دراسة Azees et al. (2016) أن التدابير المضادة (مكافح البرامج الضارة) تحد من هجمات البرامج الضارة.

وقد يعود هذا الأثر السلبي إلى استغلال الثغرات في الضوابط التقنية أو الثغرات في تكنولوجيا المعلومات، ويؤيد ذلك تقرير Citigate ICT PR (2003) الذي أشار إلى أن هجمات الاحتيال الهاتفي أصبحت أكثر تطوراً؛ حيث يستغل المهاجمون الثغرات في تقنيات الاتصالات الجديدة، ووفقاً لدراسة Kennedy (2014) استخدم المهاجمون طرقاً لاعتراض المكالمات، أو اختراق نظام البريد الصوتي، أو إتلاف المحتوى الأصلي، وأيضاً قد يرجع هذا الأثر السلبي إلى عدم تحديث مكافح البرامج الضارة باستمرار؛ أي أن الفيروسات الحديثة يمكنها إتلاف الأنظمة والبرامج واستنزاف الموارد؛ نظراً لعدم تحديث مكافح الفيروسات، وأن التحديثات التي تلغي فاعلية الفيروسات الحديثة تحتاج إلى وقت من أول ظهور لها وحتى إنتاج تحديثات مضادة لها.

الفرضية الفرعية الثامنة:

أظهرت النتائج في الجدول (10) أن المخاطر العامة لها تأثير غير دال في الضوابط الإدارية لدى شركات الاتصالات في صنعاء؛ حيث كانت قيمة معامل المسار ($\beta = 0.044$)، وقيمة ($t = 0.377$) غير دالة إحصائياً عند مستوى دلالة أقل من (0.05)، وهذه النتيجة لا تدعم صحة الفرضية الفرعية الثامنة.

وتختلف هذه النتيجة مع دراسة Schuessler (2009) التي توصلت إلى أن المخاطر تؤثر في تدابير الردع المتمثل في الامتثال للقوانين واللوائح وتطبيق سياسة الأمن، ومن جانب آخر، أشارت دراسة Straub (1990) إلى أن جهود الردع تؤدي إلى خفض إساءة الاستخدام، ويمكن الجهود العلاجية ردع إساءة الاستخدام في المستقبل، وذكرت دراسة Ahmed et al. (2017) أن عدم الكشف عن الهوية والتوعية بأمن المعلومات يحد من مخاطر الخداع أو الانتحال.

ويلاحظ أن الأثر غير دال إحصائياً، وقد يكون هذا مؤشراً على فاعلية الضوابط الإدارية المستخدمة (منها: تطبيق السياسة الأمنية وتحديثها، والامتثال للقوانين واللوائح، والتعالي من الكوارث، والوعي والإدراك، وتدقيق الأمن) في الوقاية من المخاطر العامة التي (منها: هجمات الخداع، والبرامج الضارة، وقرصنة الهاتف)، وقد يرجع اختلاف نتيجة الدراسة الحالية عن الدراسات السابقة (إلى الآتي: 1) انخفاض هذا النوع من المخاطر في شركات الاتصالات في صنعاء؛ نظراً لفاعلية الضوابط الإدارية. (2) أو

اختلاف البيئة؛ كون الدراسات السابقة أجريت في بيئات مختلفة. (3) أو اختلاف القطاع؛ كون الدراسات السابقة أجريت في قطاعات مختلفة. (4) وقد يرجع هذا الاختلاف إلى ضعف المعرفة بالضوابط الإدارية، وعدم إدراك النطاق الكامل للضوابط، وعدم اهتمام المستخدمين بالضوابط الإدارية والتركيز على الضوابط التقنية، وهذا ما أكدته دراسة Riad (2009)، وقد يرجع ذلك إلى ضعف اهتمام المختصين في مجال الأمن بالهجمات التي تستهدف العنصر البشري والتركيز على الهجمات التي يمكن مواجهتها باستخدام تقنيات متطورة، ويؤيد ذلك ما توصلت إليه دراسة Schwartz (2011)، ويدل هذا على ضعف السياسة الأمنية وتدني مستوى الوعي بأهمية الضوابط الإدارية في تأمين شركات الاتصالات في صناعة من المخاطر.

الاستنتاجات:

- بناء على نتائج اختبار الفرضيات ومناقشتها، فقد توصلت الدراسة الحالية إلى الاستنتاجات الآتية:
1. يتضح أن مصدر التأثير السلبي في الضوابط الأمنية لدى شركات الاتصالات مجتمع الدراسة ناتج عن مخاطر التوافر، يليها مخاطر السرية، ثم المخاطر العامة دون غيرها.
 2. تبين أن مصدر التأثير السلبي في الضوابط التقنية لدى شركات الاتصالات مجتمع الدراسة ناجم عن المؤشرات المرتبطة بمخاطر السرية، كالتنصت، والوصول غير المصرح به، والاصطياد الإلكتروني.
 3. تبين أن مصدر التأثير السلبي في الضوابط الإدارية لدى شركات الاتصالات مجتمع الدراسة ناجم عن المؤشرات المرتبطة بمخاطر السرية، كالأفعال المتعمدة، وضعف إدارة كلمات المرور، والهندسة الاجتماعية.
 4. تبين أن مصدر التأثير السلبي في الضوابط التقنية لدى شركات الاتصالات مجتمع الدراسة ناجم عن المؤشرات المرتبطة بمخاطر التوافر، كهجمات الحرمان من الخدمة، وأعطال الأجهزة الفنية.
 5. تبين أن مصدر التأثير السلبي في الضوابط الإدارية لدى شركات الاتصالات مجتمع الدراسة ناجم عن المؤشرات المرتبطة بمخاطر التوافر، كالكوارث الطبيعية والسياسية، وأعطال الأجهزة الفنية.
 6. تبين أن مصدر التأثير السلبي في الضوابط التقنية لدى شركات الاتصالات مجتمع الدراسة ناجم عن المؤشرات المرتبطة بالمخاطر العامة، كالبرامج الضارة، وقرصنة الهاتف، والانتحال أو الخداع.

التوصيات:

- بناء على الاستنتاجات التي تم التوصل إليها توصي الدراسة الحالية شركات الاتصالات في صناعة بالآتي:
1. ينبغي ربط استثمار الضوابط الأمنية بالأهداف الاستراتيجية للشركة، وتقييم دوري للمخاطر؛ لتحديد الثغرات الأمنية وتحديد أولويات الاستثمار، واعتماد معايير دولية، وتعزيز البعد البشري.
 2. ضرورة استخدام مصادقة متعددة العوامل، والتحكم في نقاط الوصول إلى الأنظمة والشبكات، ومراقبة التهديدات الداخلية، واختبار الاختراق؛ لكشف الثغرات الأمنية، وتشفير البيانات السرية.
 3. ينبغي أن تكون سياسة الأمن واضحة، مع الفصل بين المهام؛ للحد من مخاطر انتهاك السرية الناجمة عن الأخطاء الداخلية، ودعم الإجراءات الرقابية والتدقيق الأمني؛ لأن الضوابط الإدارية تحتاج إلى متابعة، وتنفيذ برامج التوعية والتدريب.
 4. ينبغي حماية الأنظمة من هجمات تعطل الخدمة، مثل تحديث أنظمة كشف التسلل وجدران الحماية، وإدارة دورة حياة الأجهزة، والاسترداد الفوري للبيانات والأنظمة بعد الحادث.
 5. اختبار فاعلية خطة التعافي من الكوارث والموقع البديل، والتدريب والوعي التنظيمي كالعامل عن بُعد أثناء الطوارئ، وإجراء مراجعة دورية للصلاحيات، ومراجعة خطة استمرارية العمل بشكل دوري.

6. تعزيز إجراءات حماية الأنظمة من مخاطر البرامج الضارة، والانتحال، واعتراض المكالمات، وإتلاف المحتوى، والتحقق من الثغرات التي قد توجد في تقنيات الاتصالات، والمصادقة، ومكافح البرامج الضارة، والتوقيع الرقمي، والشهادات الرقمية.
7. توصية للجهات التنظيمية وصانعي السياسات: ضرورة إنشاء مركز وطني لأمن المعلومات؛ بغرض الاستجابة لحوادث أمن المعلومات واحتوائها وتجنبها مستقبلاً، وإعداد مشروع قانون لمكافحة الجرائم الإلكترونية، وحماية البيانات الشخصية، بحيث يقدم للحكومة لمناقشته وإقراره.

المقترحات:

1. بحث الدراسة الحالية في أثر مخاطر تكنولوجيا المعلومات في الضوابط الأمنية، ويمكن إجراء مزيد من الأبحاث لاستكشاف العوامل الأخرى المؤثرة في الضوابط الأمنية، مثل موازنة الأمن، والعوامل البشرية، والتطورات التكنولوجية.
2. تم إجراء الدراسة الحالية في شركات الاتصالات، وقد تكون النتائج غير قابلة للتعميم على القطاعات الأخرى؛ لذلك نقترح توسيع نطاق البحث ليشمل قطاعات أخرى.
3. تم تصنيف الضوابط الأمنية إلى: تقنية وإدارية، ونقترح دراسة أثر الضوابط الأمنية (وفقاً لتصنيف المعهد الوطني للمعايير والتكنولوجيا NIST) في مخاطر تكنولوجيا المعلومات.

المراجع:

- الثوردة نت. (2025، 31 يوليو)، ورشة بصنعاء حول المخاطر السيبرانية وطرق الحماية من الهجمات الإلكترونية. <https://althawrah.ye/archives/1023009>
- الريبيدي، محمد علي (2010)، حماية المعلومات الحاسوبية في ظل مخاطر التكنولوجيا للعمليات المصرفية الإلكترونية: دراسة ميدانية في البنوك العاملة في اليمن، مجلة كلية التجارة والاقتصاد، 33، 45-1.
- زويلف، انغام محسن حسن (2009)، طبيعة تهديدات أمن نظم المعلومات الحاسوبية الإلكترونية: دراسة تطبيقية على شركات التأمين الأردنية، المجلة العربية للحاسبة، 12 (1)، 46-77.
- سبانت. (2014، 23 يونيو)، المؤتمر الأول لأمن المعلومات- صنعاء، المركز الوطني للمعلومات. https://yemennic.com/conferences/activ_detailsce9d.html?ID=69967
- الشوكانى، غمدان (2016، مايو 11)، أكثر من 37 مليار ريال خسائر مؤسسة الاتصالات منذ بدء العدوان، وكالة الأنباء اليمنية سبأ. <https://www.saba.ye/ar/news427488.htm>
- عدن الغد. (2014)، خلل بشبكة (MTN) يوقف حركة الاتصالات بعدن. <https://adengad.net/public/posts/103375>
- فاضل، عبدالكريم محمد يحيى (2018)، تقييم مخاطر أمن نظم المعلومات الحاسوبية المحوسبة لدى البنوك التجارية في اليمن: دراسة تطبيقية [أطروحة دكتوراه، جامعة دمشق، سوريا].
- قانون رقم (13) لسنة 2012م بشأن حق الحصول على المعلومات. (2012). الجريدة الرسمية، الجمهورية اليمنية.
- قانون رقم (40) لسنة 2006م بشأن أنظمة الدفع والعمليات المالية والمصرفية الإلكترونية. (2006)، الجريدة الرسمية، (24)، الجمهورية اليمنية.
- القحطاني، ذيب بن عايض (2015)، أمن المعلومات، الرياض، السعودية: مكتبة الملك فهد الوطنية.
- وزارة الاتصالات وتقنية المعلومات. (2020)، الاتصالات والبريد، خمسة أعوام من الصمود. https://mtit.gov.ye/co_sub_media_image/28-Arabic_2020_R2.pdf

- Ahmed, A. W., Khan, O. A., Ahmed, M. M., & Shah, M. A. (2017). A comprehensive analysis on the security threats and their countermeasures of IoT. *International Journal of Advanced Computer Science and Applications*, 8(7), 489–501. <https://doi.org/10.14569/IJACSA.2017.080768>
- Al-ghananeem, K. M. (2014). The impact of information security management standards to ensure information security. *International Journal of Economics and Research*, 5(1), 46-66.
- Al-shaibany, N. A., Al-sofi, T. A. B., & Al Gaphari, G. H. (2023). A model for enhancing the information security management systems in Yemen banks. *Sana'a University Journal of Applied Sciences and Technology*, 1(1), 1–12. <https://doi.org/10.59628/jast.v1i1.14>
- Atyam, S. B. (2010). Effectiveness of security control risk assessments for enterprises: Assess on the business perspective of security risks. *Information Security Journal: A Global Perspective*, 19(6), 343–350. <https://doi.org/10.1080/19393555.2010.514892>
- Australian Cyber Security Centre. (2015). *2015 cyber security survey: Major Australian businesses*. <https://www.cybersecurityhub.gov.au/cyberawareness/images/pdfs/2015-ACSC-Cyber-Security-Survey-Major-Australian-Businesses.pdf>
- Azees, M., Vijayakumar, P., & Jegatha Deborah, L. (2016). Comprehensive survey on security services in vehicular ad-hoc networks. *IET Intelligent Transport Systems*, 10(6), 379–388. <https://doi.org/10.1049/iet-its.2015.0072>
- Banța, V. (2012). The strategic management of risk, threats and vulnerabilities, in an informational system. *Valahian Journal of Economic Studies*, 3(1), 7–16.
- CERT Australia. (2014). *Cyber crime & security survey report 2013*. Commonwealth of Australia.
- Chin, W. W. (1998). Issues and opinion on structural equation modeling. *MIS Quarterly*, 22(1), 7–16. <https://doi.org/10.2307/249674>
- Choeje, P., Murray, D., & Fung, C. C. (2016). Exploring critical success factors for cybersecurity in Bhutan's government organizations. *Computer Science & Information Technology*, 6(15), 49–61. <https://doi.org/10.5121/csit.2016.61505>
- Citigate ICT PR. (2003, March 13). *Fraud a major threat in telecoms industry*. ITWeb.
- Committee on National Security Systems. (2015). *Committee on National Security Systems (CNSS) glossary* (CNSSI No. 4009). <https://nsarchive.gwu.edu/sites/default/files/documents/3238368/Document-08-Committee-on-National-Security.pdf>

- D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79–98. <https://doi.org/10.1287/isre.1070.0160>
- Daferighe, E. E., & Udihi, M. (2014). Computerized accounting information systems and system risk management in Nigerian banks. *International Journal of Research in Computer Application & Management*, 4(7), 67-72.
- Deloitte. (2006). *Protecting the digital assets: The 2006 technology, media & telecommunications security survey*. London: Deloitte Touche Tohmatsu Limited.
- Deloitte. (2013). *Blurring the lines: 2013 TMT global security study*. London: Deloitte Touche Tohmatsu Limited.
- Deloitte. (2014). *Global cyber executive briefing*. London: Deloitte Touche Tohmatsu Limited.
- Department for Business, Innovation & Skills. (2013). *Information security breaches survey 2013: Technical report* (BIS/13/P184). <https://www.gov.uk/government/publications/information-security-breaches-survey-2013-technical-report>
- 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. <https://doi.org/10.3233/JCS-2009-0398>
- Hair, J. F., Jr., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)* (2nd ed.). SAGE Publications.
- 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. <https://doi.org/10.1108/EBR-11-2018-0203>
- Hayale, T. H., & Abu Khadra, H. A. (2006). Evaluation of the effectiveness of control systems in computerized accounting information systems: An empirical research applied on Jordanian banking sector. *Journal of Accounting, Business and Management*, 13(1), 39–68.
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115–135. <https://doi.org/10.1007/s11747-014-0403-8>
- Horne, C. A., Ahmad, A., & Maynard, S. B. (2016). A theory on information security. In *Proceedings of the 27th Australasian Conference on Information Systems (ACIS 2016)*. University of Wollongong. <https://aisel.aisnet.org/acis2016/87/>

- International Organization for Standardization. (2009). *Information technology—Security techniques—Information security management systems—Overview and vocabulary* (ISO/IEC Standard No. 27000:2009). <https://www.iso.org/standard/41933.html>
- International Telecommunication Union. (2015). *Global cybersecurity index & cyberwellness profiles*. <https://www.itu.int/pub/D-STR-SECU-2015>
- International Telecommunication Union. (2017). *Global cybersecurity index 2017*. <https://www.itu.int/pub/D-STR-GCI.01-2017/en>
- International Telecommunication Union. (2019). *Global cybersecurity index 2018*. <https://www.itu.int/pub/D-STR-GCI.01-2018>
- International Telecommunication Union. (2021). *Global cybersecurity index 2020*. <https://www.itu.int/pub/D-STR-GCI.01-2021/en>
- International Telecommunication Union. (2024). *Global cybersecurity index 2024* (5th ed.). <https://www.itu.int/hub/publication/d-hdb-gci-01-2024/>
- Jadrić, M., Čukušić, M., & Garača, Ž. (2016). Exploring the responsibilities and practices behind information security governance. In D. Tipurić & I. Kovač (Eds.), *Proceedings of the 4th International OFEL Conference on Governance, Management and Entrepreneurship* (pp. 328–342). CIRU – Governance Research and Development Centre.
- Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments* (NIST Special Publication 800-30, Rev. 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-30r1>
- Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, 32, 489-496.
- Kaspersky. (2016, August 22). *Threat intelligence report for the telecommunications industry*. Securelist. <https://securelist.com/threat-intelligence-report-for-the-telecommunications-industry/75846/>
- Kaspersky. (2024, July 31). *Kaspersky: Telecoms are prime targets for cyberattacks in 2024*. <https://www.kaspersky.co.uk/about/press-releases/kaspersky-telecoms-are-prime-targets-for-cyberattacks-in-2024>
- Kennedy, K. (2014). *Phone phreaking history & impact on telecommunications*. Kennedy Info Sec. http://kennedyinfosec.com/blog/?page_id=547
- Kumar, R. L., Park, S., & Subramaniam, C. (2008). Understanding the value of countermeasure portfolios in information systems security. *Journal of Management Information Systems*, 25(2), 241-279. <https://doi.org/10.2753/MIS0742-1222250210>
- Lee, S. (2025, March 27). *Optimizing telecom security through effective privacy regulation steps*. Number Analytics. <https://www.numberanalytics.com/blog/optimizing-telecom-security>

- Lévy-Bencheton, C., & Darra, E. (2015). *Cyber security for smart cities: An architecture model for public transport*. European Union Agency for Network and Information Security. <https://doi.org/10.2824/846575>
- 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. <https://doi.org/10.2307/249574>
- Malyuk, A., & Miloslavskaya, N. G. (2014). *Information security theory development*. In *Proceedings of the 7th International Conference on Security of Information and Networks (SIN '14)* (pp. 52–55). Association for Computing Machinery. <https://doi.org/10.1145/2659651.2659659>
- Mbowe, J. E., Zlotnikova, I., Msanjila, S. S., & Oreku, G. S. (2014). A conceptual framework for threat assessment based on organization's information security policy. *Journal of Information Security*, 5(4), 166–177. <https://doi.org/10.4236/jis.2014.54016>
- Medina, M., Serna, J., Sfakianakis, A., Aguilá, J., & Fernández, L. Á. (2013). *eID authentication methods in e-finance and e-payment services: Current practices and recommendations*. European Union Agency for Network and Information Security. <https://doi.org/10.2824/27272>
- Muhrtala, T. O., & Ogundeji, M. (2013). Computerized accounting information systems and perceived security threats in developing economies: The Nigerian case. *Universal Journal of Accounting and Finance*, 1(1), 9–18. <https://doi.org/10.13189/ujaf.2013.010102>
- National Cyber Security Index. (2020). Yemen. https://ncsi.ega.ee/country/ye_2022/
- National Institute of Standards and Technology. (2006). *Minimum security requirements for federal information and information systems* (Federal Information Processing Standards Publication 200). <https://doi.org/10.6028/NIST.FIPS.200>
- Nhan, V. T. T., Dung, N. N. K., & Phuoc, T. (2025). A study on the impact of accounting information security controls on the effectiveness of internal controls in Vietnamese enterprises. *Journal of Open Innovation: Technology, Market, and Complexity*, 11(1), 100470. <https://doi.org/10.1016/j.joitmc.2025.100470>
- Office of Management and Budget. (2016, March 18). *Annual report to Congress: Federal Information Security Modernization Act*. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/final_fy_2015_fisma_report_to_congress_03_18_2016.pdf
- Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, 23(8), 638–646. <https://doi.org/10.1016/j.cose.2004.10.006>

- PricewaterhouseCoopers. (2014, September 30). *Managing cyber risks in an interconnected world: Key findings from the Global State of Information Security® Survey 2015*. <https://www.pwc.com/jg/en/publications/managing-cyber-risks-2015.pdf>
- Reuters. (2015). *Millions of computers may be compromised by US spyware: Report*. <https://www.telegraph.co.uk/news/worldnews/northamerica/usa/11416985/Millions-of-computers-may-be-compromised-by-US-spyware-report.html>
- Rhodes-Ousley, M. (2013). *Information security: The complete reference* (2nd ed.). 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].
- 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].
- Schuessler, J. H. (2013). Contemporary Threats Countermeasures. *Journal of Information Privacy and Security*, 9(2), 3-20.
- Schwartz, M. J. (2011, September 21). *Social engineering attacks cost companies*. Dark Reading. <https://www.darkreading.com/vulnerabilities-threats/social-engineering-attacks-cost-companies>
- Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for information technology systems* (NIST Special Publication 800-30). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-30>
- Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 22(4), 441-469. <https://doi.org/10.2307/249551>
- Straub, D. W., Jr. (1987). Controlling computer abuse: An empirical study of effective security countermeasures. *Proceedings of the 8th International Conference on Information Systems (ICIS 1987)* (pp. 277-289). Pittsburgh, Pennsylvania. <https://aisel.aisnet.org/icis1987/32/>
- Straub, D. W., Jr. (1990). Effective IS security: An empirical study. *Information Systems Research*, 1(3), 255-276. <https://doi.org/10.1287/isre.1.3.255>
- Swanson, M. M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). *Contingency planning guide for federal information systems* (NIST Special Publication 800-34 Rev. 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-34r1>

- Symantec Corporation. (2016, April). *Internet security threat report* (Vol. 21). <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>
- Tarmidi, M., Rashid, A. A., Deris, M. S. B., & Roni, R. A. (2013). Computerized accounting system threats in Malaysian public services. *International Journal of Finance and Accounting*, 2(2), 109–113.
- U.S. Government Accountability Office. (2015, July 8). *Information security: Cyber threats and data breaches illustrate need for stronger controls across federal agencies* (GAO-15-758T). <https://www.gao.gov/products/gao-15-758t>
- U.S. Government Accountability Office. (2016, May 18). *Information security: Agencies need to improve controls over selected high-impact systems* (GAO-16-501). <https://www.gao.gov/products/gao-16-501>
- Verizon. (2023). *2023 data breach investigations report*. <https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf>
- Verizon. (2025). *2025 data breach investigations report*. <https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf>
- von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
- Whitman, M. E. (2004). In defense of the realm: Understanding the threats to information security. *International Journal of Information Management*, 24(1), 43–57. <https://doi.org/10.1016/j.ijinfomgt.2003.12.003>
- Yau, H. K. (2014). Information security controls. *Advances in Robotics & Automation*, 3(2), e118.

Arabic References in Roman Scripts:

- Aden al-Ghad. (2014). *Khalal bi-shabakat (MTN) yuqif harakat al-ittisalat bi-Aden*. <https://adengad.net/public/posts/103375>
- al-Qahtani, Dhib bin Ayid (2015). *Amn al-ma'lumat*. al-Riyad, al-Su'udiyah: Maktabat al-Malik Fahd al-Wataniyyah.
- Al-Rubaydi, Muhammad Ali (2010). Himayat al-ma'lumat al-muhasabiyyah fi zill makhatir al-tiknulujiya lil-amaliyyat al-masrafiyyah al-iliktruniyyah: Dirasah maydaniyyah fi al-bunuk al-'amilah fi al-Yaman. *Majallat Kulliyyat al-Tijarah wa al-Iqtisad*, 33, 1–45.

- Al-Shawkani, Ghamdan (2016, Mayu 11). *Akthar min 37 milyar riyal khasa'ir Mu'assasat al-Ittisalat mundhu bad' al-'udwan*. Wikalat al-Anba' al-Yamaniyyah Saba. <https://www.saba.ye/ar/news427488.htm>
- Al-Thawrah Net. (2025, Yuliyu 31). *Warshah bi-Sana'a hawla al-makhatir al-sibraniyyah wa turuq al-himayah min al-hajamat al-iliktruniyyah*. <https://althawrah.ye/archives/1023009>
- Fadil, Abd al-Karim Muhammad Yahya (2018). *Taqyim makhatir amn nuzum al-ma'lumat al-muhasabiyyah al-mawsabah lada al-bunuk al-tijariyyah fi al-Yaman: Dirasah tatbiqiyyah* [Utruhah dukturah, Jami'at Dimashq, Suriya].
- Qanun raqm (13) li-sanat 2012 bi-sha'n haqq al-husul 'ala al-ma'lumat (2012). *Al-Jaridah al-Rasmiyyah*. Al-Jumhuriyyah al-Yamaniyyah.
- Qanun raqm (40) li-sanat 2006 bi-sha'n anzimat al-daf' wa al-amaliyyat al-maliyyah wa al-masrafiyyah al-iliktruniyyah (2006). *Al-Jaridah al-Rasmiyyah*, (24), Al-Jumhuriyyah al-Yamaniyyah.
- Saba Net. (2014, Yuniyu 23). *Al-mu'tamar al-awwal li-amn al-ma'lumat - Sana'a*. Al-Markaz al-Watani lil-Ma'lumat. https://yemennic.com/conferences/activ_detailsce9d.html?ID=69967
- Wizarat al-Ittisalat wa Taqniyat al-Ma'lumat. (2020). *Al-ittisalat wa al-barid: Khamsat a'wam min al-sumud*. https://mtit.gov.ye/co_sub_media_image/28-Arabic_2020_R2.pdf
- Zuwaylif, Angham Muhsin Hasan (2009). *Tabi'at tahdidat amn nuzum al-ma'lumat al-muhasabiyyah al-iliktruniyyah: Dirasah tatbiqiyyah 'ala sharikat al-ta'min al-Urduniyyah*. *Al-Majallah al-Arabiyyah lil-Muhasabah*, 12(1), 46–77.