مستوى أمن المعلومات في قطاع الاتصالات باليمن

الاستلام: 12/يونيو/2022
التحكيم: 24/يونيو/2022
القبول: 4/أغسطس/2022

نبيل حسان عبده الحميري [1,*]

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

http://doi.org/10.59222/ustjmhs.1.1.1

مستوى أمن المعلومات في قطاع الاتصالات باليمن

الملخص:

هدفت الدراسة إلى تحديد مستوى أمن المعلومات (السرية، والسلامة، والتوافر) في قطاع الاتصالات باليمن؛ ولتحقيق هذا الهدف، تم استخدام المنهج الوصفي، والاعتماد على الاستبانة في جمع البيانات من عينة الدراسة وفقا لأسلوب الحصر الشامل في قطاع الاتصالات الذي شمل شركات الاتصالات الست والمؤسسة العامة للاتصالات، وتم توزيع الاستبانة على (356) مشاركا، وجمعت فقط (218) استمارة كانت صالحة للتحليل، وتم تحليل البيانات باستخدام برنامج الحزمة الإحصائية في العلوم الاجتماعية (SPSS)، وقد أشارت نتائج الدراسة إلى أن مستوى أمن المعلومات في قطاع الاتصالات باليمن مرتفع؛ حيث جاء مستوى السرية الأعلى، يليها السلامة، ثم التوافر، وأوصت الدراسة: بضرورة تعزيز أمن المعلومات، ودعم إجراءات حماية المعلومات من الكشف أو التعديل، ودعم أنشطة الوصول المصرح به إلى المعلومات والخدمات.

الكلمات المفتاحية: أمن المعلومات، قطاع الاتصالات، اليمن.

http://doi.org/10.59222/ustjmhs.1.1.1

Degree of Information Security at Telecommunications Sector in Yemen

Abstract:

This study aimed to determine the degree of information security (confidentiality, integrity, availability) at telecommunications sector in Yemen. To achieve this, the descriptive method was followed and a questionnaire was used for collecting data from the study sample at telecommunications sector, which includes the six telecommunication companies and Public Telecom Corp. The sample was selected by the complete census method. The questionnaire forms were distributed to (356) participants; however, only (218) forms were valid for analysis. The data were analyzed by the Statistical Package for the Social Sciences (SPSS) program. The study findings revealed that the degree of information security at telecommunications sector in Yemen was high; the degree of confidentiality was the highest, followed by integrity, then availability. The study recommended that the information security should be reinforced, and procedures for protecting information from disclosure or modification, as well as activities for authorized access to information and services should be supported.

Keywords: information security, telecommunication sector, Yemen.

http://doi.org/10.59222/ustjmhs.1.1.1

المقدمة:

تحظى قضايا أمن المعلومات باهتمام كبير من قبل المنظمات، وتُعد سرية المعلومات وسلامتها وتوافرها من القضايا المهمة في جميع القطاعات، بما في ذلك قطاع الاتصالات؛ كون هذا القطاع يسيطر ويشغل البنية التحتية الحيوية التي تُستخدم على نطاق واسع في التواصل، وتخزين كميات كبيرة من البيانات الحساسة (Deloitte, 2014, 16)، ونظرا لأهمية أمن المعلومات في منظمات الأعمال، فقد أصدرت الهيئات المهنية، مثل COBIT وISO وNIST أطرا ومعايير تساعد في حماية المعلومات ورفع مستوى أمن المعلومات، وذلك من خلال كشف وخفض الحوادث الأمنية، وتأمين البيانات الحساسة، وإدراك الثغرات في السياسة (Hulme, 2015)، وأصدرت الجهات الرسمية قوانين، مثل: قانون مكافحة الجرائم الإلكترونية، وقانون حماية البيانات الشخصية، وقانون ساربنيز-اوكسلي (SOX) التي تساعد في تحقيق أمن المعلومات، وتحسين مستوى أمن المعلومات، وذلك من خلال تجريم ومعاقبة الوصول غير المشروع إلى أنظمة المعلومات، وتشديد العقوبة على المخالفين (AlKalbani, Deng, Kam, & Zhang, 2017, 104).

وقد تناولت بعض الدراسات (Chang & Wang, 2011; Mohammad, Awadhi, Kananah, & Job, 2012; Seno, Bidmeshk, & Ghaffari, 2015) القضايا المتعلقة بتأمين المعلومات من الكشف، والحفاظ على خصوصية العملاء، والرقابة على عمليات الوصول إلى المعلومات، وكشف التعديلات التي قد تحدث في المعلومات والأنظمة، واستمرارية العمل عند انقطاع الطاقة، والوصول إلى المعلومات والأنظمة والخدمات عند الطلب.

وقد أشارت دراسة Neogy (2014، 48) إلى وجود مخاطر في شركات اتصالات الهاتف النقال في بنجلاديش، وذكرت دراسة Richardson (2010، 15-17) العديد من الهجمات التي عانت منها أنظمة الشركات، ووجدت دراسة Deloitte (2006، 3) أن المخاطر في شركات الاتصالات زادت بشكل عام، وأكد تقرير Deloitte (2014، 16) أن استهداف شركات الاتصالات زاد، مثل: التنصت على خطوط الهاتف، والدردشة عبر الإنترنت، والوصول إلى البيانات الشخصية، والوصول إلى خدمات مكلفة مثل المكالمات الدولية.

وقد أثرت الاختراقات الأمنية في الأنشطة التجارية، وأدت إلى حدوث خسائر مالية كبيرة، وتوقف أنظمة، وفقدان إيرادات، وإلحاق أضرار كبيرة بسمعة الشركة، وفقدان الثقة بها (Deloitte, 2014, 16)؛ حيث أكدت دراسة Whitman (2004، 51) أن مزودي خدمات الاتصالات والطاقة هم الأكثر تأثرا بتوافر الخدمة وأمن المعلومات، وكشف تقرير Kaspersky (2016، 4-5) عن تضرر مزودي خدمات قطاع الاتصالات في جميع أنحاء العالم أكثر من أي قطاع آخر والناتج عن الهجمات السيبرانية، وذكر تقرير Deloitte (2014، 16) أن قنوات الاتصال تُعد هدفا للهجمات التي تستهدف المعلومات السرية؛ حيث أشارت دراسة Deloitte (2006، 3) إلى أن ثلث الاختراقات التي عانت منها شركات الاتصالات أدت إلى حدوث خسائر مالية كبيرة، وإلحاق أضرار بسمعة الشركة والعلامة التجارية، وتوقف النظام، وفقدان إيرادات، وأكد تقرير Deloitte (2014، 16) أن الهجمات التي استهدفت شركات الاتصالات أدت إلى إلحاق أضرار كبيرة بسمعة الشركات وسرية المعلومات؛ حيث أثارت مخاوف العملاء المتعلقة بالخصوصية، وبالتالي أدت إلى فقدان الثقة.

وقد أشار الاستطلاع العالمي لأمن المعلومات (Ernst & Young, 2012, 9) إلى أن الفجوة الأمنية تتسع باستمرار بين المستوى الحالي والمستوى المطلوب لأمن المعلومات، وأرجع تقرير مكتب المساءلة الحكومية (GAO, 2016a, 6) اتساع الفجوة المستمرة إلى نقاط الضعف (الثغرات الأمنية)، أو عدم مواكبة أمن المعلومات للتغيرات المتسارعة في بيئة الأعمال (Riad, 2009, 14)، أو عدم كفاية إدارة أمن المعلومات (Kankanhalli, Teo, Tan, &Wei, 2003, 139)، أو عدم كفاية الأمن الإلكتروني (International Telecommunication Union (ITU), 2014, 3).

http://doi.org/10.59222/ustjmhs.1.1.1

وبالتالي، لاتزال قضايا أمن المعلومات تثير قلق المنظمات، وتشكل تحديا كبيرا لها (Riad, 2009, 35)؛ حيث أجمع ثلث المختصين في مجال تكنولوجيا المعلومات على أن منع الاختراقات الأمنية تشكل الهم الأكبر للمنظمات وفق ما جاء في تقرير Kaspersky (يحيى، 2012)، وأن أكثر من ثلث المنظمات لا تزال تفتقر إلى الثقة في قدرة أمن المعلومات على كشف الهجمات المتطورة، كما أن الغالبية العظمى من المشاركين يعتقدون أن أمن المعلومات لا يلبي تماما احتياجات منظماتهم (Bernews, 2015).

ويمثل قطاع الاتصالات في اليمن مكونا أساسيا ومهما في البنية التحتية الحيوية، وكذلك دوره يُعد مهما في تعزيز النمو الاقتصادي، وأحد أهم المصادر الإيرادية للدولة، ويُسهم في توفير مزيد من فرص العمل (البشيري، 2021). وتُعد سرية المعلومات وسلامتها وتوافرها في قطاع الاتصالات قضية جوهرية، وأي كشف عن المعلومات السرية أو تعديلها أو عدم توافرها سيؤثر سلبا في أمن المعلومات بقطاع الاتصالات، وبالتالي سيؤثر في سمعة الشركة ويثير قلق العملاء (Deloitte, 2014, 16).

أمن المعلومات:

إن أمن المنظمة نظام متعدد الطبقات يحمي أصولها، ومواردها، وعملياتها، ويجب أن يكون للمنظمات الناجحة طبقات أمنية متعددة، مثل: الأمن المادي، وأمن الأفراد، وأمن العمليات، وأمن الاتصالات، وأمن الشبكات، وأمن المعلومات (Whitman & Mattord, 2011, 8)، وتزداد الحاجة إلى أمن المعلومات مع تطور الهجمات المستمرة التي تستهدف سرية المعلومات، وسلامتها، وتوافرها (Donaldson, Siegel, Williams, & Aslam, 2015, 10).

أولا: مفهوم أمن المعلومات:

أصبح استخدام مصطلح أمن المعلومات شائعا بعد ظهور أنظمة وتكنولوجيا المعلومات والاتصالات، واستخدامها على نطاق واسع في معالجة البيانات، ونقلها، وتخزينها، وقد عرّف المعهد الوطني للمعايير والتكنولوجيا (Paulsen & Toth, 2016, 2) أمن المعلومات بأنه: حماية المعلومات من الوصول غير المصرح به، أو الكشف، أو التعديل، أو الإتلاف، وجعل المعلومات متاحة لمستخدميها بشكل دائم من أجل ضمان: السرية، والسلامة، والتوافر، وعرّفتها المنظمة الدولية للمعايير (ISO/IEC JTC 1, 2018, 4) بأنها: الحفاظ على سرية المعلومات، وسلامتها، وتوافرها، وعرّفتها جمعية تدقيق ورقابة نظم المعلومات (Information Systems Audit and Control Association (ISACA), 2012, 38) بأنها: ضمان حماية المعلومات داخل المنظمة من الكشف غير المصرح به (السرية)، والتعديل غير المشروع (السلامة)، ورفض الوصول عند الطلب (التوافر).

ولأغراض الدراسة الحالية فإن تعريف أمن المعلومات هو الحفاظ على سرية المعلومات، وسلامتها، وتوافرها سواء أثناء المعالجة، أو التخزين، أو النقل.

ثانيا: أهمية أمن المعلومات:

أدى انتشار أنظمة وشبكات المعلومات والاعتماد عليها إلى عدم إهمال القضية الأمنية من قبل أي نشاط تجاري (Riad, 2009, 35)، وقد استثمرت الشركات في مجال أمن المعلومات وتطبيقات الأعمال التجارية (Brown et al., 2012, 32)؛ وذلك لضمان السرية، والسلامة، والتوافر في جميع مراحل دورة حياة المعلومات (Joint Task Force Transformation Initiative, 2013, 1)، ويُعد قطاع الاتصالات أكثر القطاعات إنفاقا على أمن المعلومات، يليه قطاع الخدمات، ثم قطاع التكنولوجيا (PricewaterhouseCoopers (PwC) & Infosecurity, 2015, 36).

وكذلك تحتل قضايا أمن المعلومات مساحة واسعة من الدراسات والأبحاث وعقد المؤتمرات؛ حيث أشار تقرير الأمن السيبراني (Cisco, 2015, 48) المختص بأمن المعلومات إلى أن ثلثي المستجيبين (مدراء العمليات الأمنية، وكبار موظفي أمن المعلومات) يرون أن القيادة التنفيذية في منظماتهم تعتبر الأمن أولوية عالية، ووجدت دراسة جرائم وأمن الحاسوب (Richardson, 2010, 32) أن نصف

http://doi.org/10.59222/ustjmhs.1.1.1

المستجيبين يرون أن الإدارة العليا تعتبر الأمن أولوية عالية، وأشارت دراسة اختراقات أمن المعلومات (ISBS, 2014, 4) إلى أن أولوية أمن المعلومات عالية في الشركات، وأكد غالبية المشاركين على أهمية أمن المعلومات وأولويته وأثره الإيجابي في أنظمة الشركات، أيضا تتزايد أهمية الأمن؛ لأن جزءا كبيرا من الاقتصاد العالمي انتقل إلى الفضاء السيبراني، وأصبحت حماية وضمان تدفق البيانات عبر هذه الشبكات لها أولوية (Lehto & Neittaanmäki, 2022)، وأولوية قطاع الاتصالات تتمثل في حماية الشبكات، والكم الهائل من البيانات، والمرافق من الوصول غير المصرح به أو الاعتراض؛ لضمان توافر وسلامة شبكات ومرافق الاتصالات وسرية الاتصالات والمعلومات (Berisha & Tawfik, 2016).

ثالثا: أبعاد أمن المعلومات:

يُقصد بأمن المعلومات الحفاظ على سرية المعلومات وسلامتها وتوافرها أثناء المعالجة أو التخزين أو النقل (ISO/IEC JTC 1, 2018, 4; Paulsen & Toth, 2016, 2; ISACA, 2012, 38)، ويتحقق أمن المعلومات من خلال تصميم وتنفيذ الضوابط الأمنية الملائمة التي تعمل على حماية المعلومات من الكشف، والتعديل، وإتاحة المعلومات للمستخدمين بشكل دائم، ومنع أو كشف أو الحد من الوصول غير المصرح به إلى الحواسيب والبرامج والمرافق (GAO, 2016b, 44)، ويتضمن هذا التعريف أبعاد أمن المعلومات المتمثل في السرية، والسلامة، والتوافر، ومن خلال هذه الأبعاد الثلاثة يتم قياس مستوى أمن المعلومات، وتوضيحها كالآتي:

1. سرية المعلومات: تعني حماية المعلومات من الكشف والاستخدام غير المصرح به (Peltier, 2014, 14)، ويشير عنصر السرية إلى أن كافة المعلومات الحساسة المتعلقة بالشركة وعملائها محمية من الكشف والوصول غير المصرح به، ويتم الحفاظ على سرية المعلومات طوال دورة حياتها، وفي جميع مراحلها بما في ذلك: تخزينها، ومعالجتها، ونقلها (ISO/IEC JTC 1, 2011, 40)، ويتم قياس مستوى سرية المعلومات من خلال الفقرات التسع المذكورة في الجدول (2).
2. سلامة المعلومات: تعني المحافظة على تطابق البيانات ودقتها؛ مما يمنع تعديل وإتلاف البيانات المتعمد أو غير المتعمد من قبل أطراف غير مصرح لها (Norman, Hamid, Hanifa, & Tamrin, 2017, 2)، وتشير سلامة المعلومات إلى سلامة البرامج والأجهزة المستخدمة في تبادل المعلومات ومعالجتها وتخزينها (ISO/IEC JTC 1, 2011, 40)، وتتحقق السلامة عندما تبقى البيانات دون تعديل من وقت إدخالها إلى النظام حتى استرجاعها لاحقا (Donaldson et al., 2015, 12)، ويتم قياس مستوى سلامة المعلومات من خلال الفقرات التسع المذكورة في الجدول (2).
3. توافر المعلومات: تعني ضمان الوصول إلى المعلومات عند الطلب، والوثوق بها، واستخدامها (Kissel, 2013, 17)، وهذا يتطلب جعل أنظمة المعلومات متاحة لمستخدميها بشكل دائم (حجر، 2014)، ويتحقق عنصر التوافر من خلال حماية الشبكة والأجهزة والأنظمة والبرامج من التوقف أو الكوارث المعلوماتية (القحطاني، 2015)، ويتم قياس مستوى توافر المعلومات من خلال الفقرات العشر المذكورة في الجدول (2).

الدراسات السابقة:

تناولت الدراسات السابقة العديد من العوامل التي تؤثر في أمن المعلومات، كالمخاطر والضوابط الأمنية؛ حيث ذكرت دراسة Riad (2009) أن بعض العوامل تؤثر بشكل سلبي في أمن المعلومات كالمخاطر، وأن التكنولوجيا هي أحد العوامل المؤثرة في أمن المعلومات التي قد تؤثر بشكل إيجابي في أمن المعلومات من خلال تعزيز القدرات الأمنية، وقد تؤثر التكنولوجيا أيضا بشكل سلبي في أمن المعلومات من خلال استحداث ثغرات أمنية جديدة، وأشار Berisha وTawfik (2016) إلى أن المخاطر التي تواجه قطاع الاتصالات تتمثل في اعتراض حركة مرور البيانات في الشبكة من قبل الموظفين غير المصرح لهم، أو إجراء تغييرات غير قانونية في الملفات الشخصية لمستخدمي الشبكة ونظام الفوترة؛ مما يسبب إجراء مكالمات مجانية وفقدان المصداقية، أو الوصول غير المشروع إلى معلومات العملاء الشخصية

http://doi.org/10.59222/ustjmhs.1.1.1

والسرية، أو حجب الخدمة وتوقف حركة مرور البيانات في الشبكة، وقد تؤدي هذه الهجمات إلى خسائر مالية، والإضرار بالسمعة، وفقدان موثوقية العملاء، وعقوبات قانونية، وكشف تقرير McAfee Enterprise (2016، 55–56) عن تعرض قطاع لاتصالات في أوروبا لخسائر كبيرة ناتجة عن اختراق بيانات TalkTalk أدى إلى تحول أكثر من (100,000) عميل إلى مشغلين آخرين، وذكر تقرير FISMA (2016، 14) أن الحكومة الاتحادية شهدت زيادة ملحوظة في عدد الحوادث الأمنية التي أثرت في سرية المعلومات، وسلامتها، وتوافرها، وأكد تقرير GAO (2016a، 6) أن نقاط الضعف لا تزال تشكل تحديا يواجه مؤسسة تأمين الودائع الاتحادية في الجوانب المتعلقة بسرية المعلومات، وسلامتها، وتوافرها، ووجدت دراسة Trend Micro (2015، 18) أن 60 % من نقاط الضعف تؤثر في السرية، و30 % من نقاط الضعف تؤثر في السلامة، و10 % من نقاط الضعف تُستغل في الهجوم ضد عنصر التوافر، وأشارت دراسة CERT-AU و Australian Cyber Security Centre (ACSC) (2015، 1) إلى أن نصف المنظمات الأسترالية عانت من حوادث أمنية أثرت سلبا في سرية، وسلامة، وتوافر المعلومات، وتوصل تقييم مركز الأمن السيبراني إلى أن مستوى تهديد التجسس السيبراني ضد قطاع الاتصالات في الدنمارك انخفض من مرتفع إلى متوسط، غير أن مستوى نشاط الهجمات السيبرانية ارتفع من منخفض إلى متوسط، وأن خطر الجرائم السيبرانية مرتفع جدا (Centre for Cybersecurity, 2022).

وذكرت دراسة Riad (2009، 45) أن الضوابط الأمنية تؤثر بشكل إيجابي في أمن المعلومات، وقد أشارت دراسة Chang وWang (2011، 588) إلى أن موارد نظم المعلومات (التكنولوجية، والعلائقية، والبنية التحتية) تؤثر بشكل إيجابي في أمن المعلومات، وخلصت دراسة Seno et al. (2015، 7) إلى أن أمن المعلومات لها علاقة قوية ومباشرة بتدابير أمن المعلومات، وقد وجدت دراسة Al-ghananeem (2014، 63) أن معايير إدارة أمن المعلومات (الضوابط، والسياسات) لها تأثير إيجابي في ضمان أمن المعلومات، وذكرت دراسة Al-ghananeem ، Al-taee وJida (2014، 99–97) أن أهداف أمن المعلومات لها تأثير إيجابي في ضمان أمن المعلومات (الضوابط الأمنية)، وأظهرت دراسة Schuessler (2009، 63) أن التدابير المضادة ترتبط بشكل إيجابي بفاعلية أمن نظم المعلومات، وأشار Berisha وTawfik (2016) إلى أن تطبيق المعيار ISO/IEC 27001 داخل قطاع الاتصالات يضمن سرية خدمات الاتصالات وسلامتها وتوافرها واستعادتها، ويحقق مستويات عالية من الأمان والموثوقية، وخفض مستوى المخاطر، وتحسين نظام إدارة أمن المعلومات.

ومما سبق، نجد أن بعض الدراسات تناولت العوامل التي تؤثر سلبا في أمن المعلومات: (السرية، والسلامة، والتوافر)، والعواقب المترتبة على الهجمات، والعوامل التي تؤثر بشكل إيجابي في أمن المعلومات، ودور المعايير في تحقيق أمن المعلومات، وبالتالي، فإن الدراسة الحالية تختلف عن الدراسات السابقة في الآتي: 1) تناولت الدراسة الحالية مستوى أمن المعلومات. 2) إجراء الدراسة الحالية في البيئة اليمنية. 3) تطبيق الدراسة الحالية على قطاع الاتصالات.

مشكلة الدراسة:

تعاني اليمن من تدني مستوى الأمن السيبراني الناتج عن القصور في الجوانب التنظيمية والتشريعية؛ حيث أشارت تقارير الرقم القياسي العالمي للأمن السيبراني Global Cybersecurity Index (GCI) -الصادرة عن الاتحاد الدولي للاتصالات- إلى أن رقم اليمن القياسي في مجال الأمن السيبراني متدن جدا (International Telecommunication Union (ITU) & ABIresearch, 2015, 1-6, 30; ITU, 2017, 65; ITU, 2019, 68; ITU, 2021, 68). وكذلك أعطت أكاديمية الحوكمة الإلكترونية e-Governance Academy (eGA) اليمن درجة متدنية جدا في مجال الأمن الإلكتروني وكان ترتيبها (148) من أصل (160)، ومؤشر الأمن السيبراني الوطني (7.79) National Cyber Security Index, 2020). وكما أكد نائب رئيس الوزراء وزير الاتصالات اليمني في المؤتمر الأول لأمن المعلومات بصنعاء يونيو 2014م، أن اليمن لا يملك تشريعا يحفظ للناس خصوصياتهم ويحمي ممتلكاتهم، وأكد مدير

http://doi.org/10.59222/ustjmhs.1.1.1

المؤسسة العامة للاتصالات على أهمية إنشاء مركز وطني لأمن المعلومات يهدف إلى الاستجابة لحوادث أمن المعلومات والتعاون مع مراكز أمن المعلومات الدولية في احتواء الحوادث وتجنبها مستقبلا (سبأ نت، 2014).

وتناولت بعض الدراسات مخاطر أمن نظم المعلومات في قطاع المصارف؛ حيث توصلت دراسة الربيدي (2010) إلى وجود مخاطر تكنولوجية متوسطة في العمليات المصرفية الإلكترونية في اليمن تواجه الوصول المصرح به، وسلامة تجهيز البيانات، وخصوصية العملاء، وتخزين البيانات والبرامج. وخلصت دراسة فاضل (2018) إلى وجود مخاطر في البنوك التجارية العاملة في اليمن بدرجات متفاوتة تهدد سلامة وتكامل تجهيز البيانات، وخصوصية بيانات العملاء، وسرية المعلومات، وإتاحة النظم، وعدم الإنكار.

وكشفت بعض التقارير والدراسات عن اختراقات وحوادث أمنية عانى منها قطاع الاتصالات في اليمن؛ حيث رصد الخبراء في شركة Kaspersky المختص بأمن المعلومات تنصت وكالة الأمن القومي National Security Agency (NSA) على الحواسيب الشخصية المصابة ببرامج التجسس في (30) دولة ومن ضمنها اليمن. وقد استهدفت برامج التجسس الإلكترونية قطاع الاتصالات، وذلك من خلال وضع تعليمات برمجية في محرك الأقراص المنتجة من قبل كبرى الشركات الإلكترونية في الولايات المتحدة (Reuters, 2015). وفي تاريخ 2014/4/30م حدث خلل فني أثناء الصيانة في إحدى شركات الاتصالات العاملة في اليمن، مما أدى إلى توقف خدمة الاتصالات لساعات، وتسبب ذلك في فقدان إيرادات واستياء المشتركين من توقف الخدمة التي عطلت أعمال الكثير منهم (عدن الغد، 2014).

وقد أثرت الاختراقات والحوادث الأمنية في سرية المعلومات وسلامتها وتوافرها، وأدت إلى انقطاع الخدمات، وتوقف الأعمال، وإلحاق أضرار بالسمعة، وفقدان ثقة العملاء؛ حيث أشار التقرير الصادر عن المؤسسة العامة اليمنية للاتصالات إلى أن إجمالي خسائر قطاع الاتصالات تقدر بـ (37) مليار ريال من مارس 2015م وحتى فبراير 2016م، والناجم عن الكوارث السياسية التي أدت إلى توقف العديد من الخدمات، وفقدان إيرادات الهاتف الثابت والإنترنت، وإيراد إيجار قنوات، وفقدان إيجار مساحات هوائيات وقنوات، وخدمة استضافة المواقع، والواي ماكس، وتكاليف الصيانة والإصلاح، أيضا ذكر التقرير أن من أهم الصعوبات التي تواجه قطاع الاتصالات في اليمن هو استمرار عمل وتشغيل تجهيزات القوى والتكييف على المولدات والبطاريات على مدى (24) ساعة في اليوم؛ نظرا للانعدام الكلي للطاقة العمومية ما ينذر بتوقف الخدمات (الشوكاني، 2016).

وقدرت خسائر قطاع الاتصالات في اليمن خلال فترة الحرب حتى مارس 2020م (4.1) مليار دولار، تمثلت في تدمير البنى التحتية للقطاع من منشآت وأبراج ومحطات اتصال وسنترالات، وعدم توفر الوقود، والانعدام الكلي للطاقة العمومية، وعدم استخدام تقنية الجيل الرابع، وقد تسبب ذلك في التأثير على سلامة المعلومات وخدمات الاتصالات وتوافرها، أيضا انقطاع الكابل البحري الرئيسي تسبب في توقف الخدمات وإحداث شلل في المعاملات التجارية والحوالات المالية الداخلية والخارجية (البشيري، 2021، 11-13).

وتوصلت الدراسة الاستطلاعية التي قام بها الباحث إلى وجود مخاطر تهدد أمن المعلومات في قطاع 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، والكوارث السياسية، والانعدام الكلي للطاقة العمومية.

http://doi.org/10.59222/ustjmhs.1.1.1

ويلاحظ أن التقارير السابقة التي تناولت الأمن السيبراني في اليمن اعتمدت في تحديد الرقم القياسي العالمي للأمن السيبراني (GCI)، ومؤشر الأمن السيبراني الوطني (NCSI) على جمع المعلومات المتعلقة بالقوانين، واللوائح، وفريق الاستجابة لحالات الطوارئ والحوادث، والسياسات العامة، والاستراتيجيات الوطنية، والمعايير، والتدريب المهني وزيادة الوعي، غير أن الدراسة الحالية اعتمدت في تحديد مستوى أمن المعلومات في قطاع الاتصالات باليمن على جمع المعلومات المتعلقة بسرية المعلومات وسلامتها وتوافرها في قطاع الاتصالات باليمن.

وكما أن تحديد مستوى أمن المعلومات (السرية، والسلامة، والتوافر) في قطاع الاتصالات باليمن يساعد في تشخيص جوانب الضعف والقصور في منظومة أمن المعلومات، وتقييمها، ومعالجتها لضمان سرية المعلومات، وسلامتها، وتوافرها، لذلك، تسعى الدراسة الحالية إلى الإسهام في تحديد مستوى أمن المعلومات في قطاع الاتصالات باليمن.

أسئلة الدراسة:

بناء على مشكلة الدراسة يمكن صياغة السؤال الآتي:

ما هو مستوى أمن المعلومات (السرية، والسلامة، والتوافر) في قطاع الاتصالات باليمن؟ وسيتم الإجابة عن هذا السؤال من خلال الإجابة عن الأسئلة الفرعية الآتية:

1) ما هو مستوى سرية المعلومات في قطاع الاتصالات باليمن؟
2) ما هو مستوى سلامة المعلومات في قطاع الاتصالات باليمن؟
3) ما هو مستوى توافر المعلومات في قطاع الاتصالات باليمن؟

أهداف الدراسة:

بناء على أسئلة الدراسة تم صياغة الهدف الآتي:

تحديد مستوى أمن المعلومات (السرية، والسلامة، والتوافر) في قطاع الاتصالات باليمن. ويتفرع هذا الهدف إلى مجموعة من الأهداف الفرعية الآتية:

1) تحديد مستوى سرية المعلومات في قطاع الاتصالات باليمن.
2) تحديد مستوى سلامة المعلومات في قطاع الاتصالات باليمن.
3) تحديد مستوى توافر المعلومات في قطاع الاتصالات باليمن.

أهمية الدراسة:

تتمثل أهمية الدراسة في الآتي:

1) قدمت الدراسة الحالية أداة لقياس مستوى أمن المعلومات في قطاع الاتصالات باليمن.
2) تسهم الدراسة الحالية إسهاما عمليا في رفع مستوى أمن المعلومات في قطاع الاتصالات وتلافي جوانب الضعف والقصور والحفاظ على سرية المعلومات وسلامتها وتوافرها.
3) إمكانية استفادة مجلس الإدارة، والإدارة التنفيذية في شركات الاتصالات والمؤسسة العامة للاتصالات من نتائج الدراسة، وذلك من خلال معرفة مستوى أمن المعلومات وجوانب القصور وإنشاء إدارة لأمن المعلومات تعمل على بناء وتطبيق نظام لإدارة أمن المعلومات وفق معايير دولية.
4) إمكانية استفادة إدارة تكنولوجيا المعلومات وإدارة التدقيق الفني من نتائج الدراسة في تقييم أمن المعلومات.

http://doi.org/10.59222/ustjmhs.1.1.1

منهجية الدراسة وإجراءاتها:

منهج الدراسة:

اعتمدت الدراسة على المنهج الوصفي، وتم استخدام أساليب الإحصاء الوصفي في تحديد مستوى أمن المعلومات: (السرية، والسلامة، والتوافر) في قطاع الاتصالات باليمن.

مجتمع وعينة الدراسة:

استهدفت الدراسة الحالية قطاع الاتصالات في اليمن والذي شمل المؤسسة العامة للاتصالات وشركات الاتصالات الست (تيليمن، يمن نت، إم تي إن، سبأفون، يمن موبايل، واي) وفقا لأسلوب الحصر الشامل، ويتكون مجتمع الدراسة المستهدف من (356) مشاركا يشملك المدراء، ورؤساء الأقسام، والمشرفين، والمختصين المعنيين بأمن المعلومات في إدارة تكنولوجيا المعلومات، وإدارة التدقيق الفني، وإدارة الرقابة والتحكم، وإدارة تشغيل الشبكة والإنترنت المتواجدة في المراكز الرئيسية لشركات الاتصالات والمؤسسة العامة للاتصالات في العاصمة صنعاء، وتم استبعاد فروع هذه الشركات في بقية المحافظات؛ كون الكوادر الفنية ذات المهارات العالية تتواجد في المراكز الرئيسية، وتم جمع المعلومات عن قطاع الاتصالات مجتمع الدراسة من خلال النزول الميداني، والرجوع إلى المختصين في إدارة الموارد البشرية، ومواقع الـ Web الخاص بشركات الاتصالات، وكتاب الإحصاء السنوي الصادر عن الجهاز المركزي للإحصاء، وقد تم اختيار هذه القطاع كمجتمع للدراسة الحالية؛ نظرا لأهمية أمن المعلومات وحساسيتها في قطاع الاتصالات بشكل خاص، واعتمادها على تكنولوجيا المعلومات بشكل كبير. ويوضح الجدول (1) حجم المجتمع والعينة ونسبة الاستجابة.

جدول (1): حجم المجتمع والعينة ونسبة الاستجابة

م	الشركة	الاستبانات			الاستبيانات الصالحة للتحليل في كل من إدارة					نسبة الاستجابة
		الموزعة	المستردة	الصالحة للتحليل	تكنولوجيا المعلومات	التدقيق الفني	الرقابة والتحكم	تشغيل الشبكة والإنترنت	الإجمالي	
1	شركة A	92	81	79	28	3	7	41	79	% 86
2	شركة B	50	25	24	9	2	3	10	24	% 48
3	شركة C	66	54	52	24	4	5	19	52	% 79
4	شركة D	30	22	22	12	2	2	6	22	% 73
5	شركة E	52	16	16	5	1	0	10	16	% 31
6	شركة F	45	20	17	8	0	4	5	17	% 38
7	شركة 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	% 61	

ملاحظة: تم ترميز شركات الاتصالات بناء على طلب بعض الإدارات خوفا من التأثير السلبي المحتمل على الشركات.

وقد تم توزيع الاستبانة على جميع عناصر المجتمع عدد (356) استبانة من خلال النزول الميداني والموارد البشرية ومتعاونين، وتم استرداد (226) استبانة بنسبة 63 %، وقد كان عدد الاستبانات الصالحة للتحليل (218) استبانة بنسبة 61 % من الاستبانات الموزعة، أما الاستبانات التي لم تسترد فعددها (130) استبانة بنسبة 37 % من الاستبانات الموزعة، ويرجع ارتفاع نسبة عدم الاستجابة إلى قلق بعض الموظفين من تقديم المعلومات اللازمة للدراسة؛ كونها باعتقادهم سرية التي قد تؤدي إلى الدعاية السلبية للشركة. والجدول (1) يوضح معدلات الاستجابة بتفصيل أكثر.

http://doi.org/10.59222/ustjmhs.1.1.1

وحدة التحليل:

وحدة التحليل في الدراسة الحالية تتمثل في المنظمة (قطاع الاتصالات في اليمن)؛ كون مستوى أمن المعلومات يقاس على مستوى المنظمة.

أداة الدراسة:

تم تطوير أداة الدراسة (الاستبانة) المستخدمة في جمع البيانات عن مستوى أمن المعلومات بالاعتماد على دراسة كل من Chang وWang (2011)، Al-ghananeem et al. (2014)، **و**Seno et al. (2015)، **وتم قياس مستوى أمن المعلومات من خلال بُعد السرية الذي تضمن** 9 **فقرات، وبُعد السلامة الذي تضمن** 9 **فقرات، وبُعد التوافر الذي تضمن** 10 **فقرات وفقا لمقياس ليكرت السباعي** (Chang & Wang, 2011; Kankanhalli et al., 2003)، **حيث تشير** (7) "**موافق بشدة**" **إلى أن مستوى أمن المعلومات في قطاع الاتصالات مرتفع جدا، وتشير** (6) **إلى "مرتفع"، وتشير** (5) **إلى "مرتفع إلى حد ما"، وتشير** (4) **إلى "متوسط"، وتشير** (3) **إلى "منخفض إلى حد ما"، وتشير** (2) **إلى "منخفض"، ويشير** (1) "**غير موافق بشدة**" **إلى أن مستوى أمن المعلومات في قطاع الاتصالات منخفض جدا، ويُبين الجدول** (2) **أبعاد وفقرات أمن المعلومات.**

جدول (2)**: أبعاد أمن المعلومات وفقراتها**

الأبعاد	عدد الفقرات	م	الفقرات تقيس الفقرات الآتية مستوى أمن المعلومات في قطاع الاتصالات.
السرية	9	1	المعلومات الحساسة في الشركة محمية من الكشف.
		2	خصوصية المعلومات الشخصية للعملاء محمية من الكشف.
		3	المعلومات المنقولة عبر الشبكة محمية من الاعتراض.
		4	حسابات المستخدمين على صفحات الويب الخاصة بالشركة محمية من الكشف.
		5	يتم الوصول إلى المعلومات من قبل موظفي الشركة بحسب صلاحيتهم.
		6	تفرض الشركة رقابة صارمة على الوصول المادي إلى الخوادم ووسائط التخزين.
		7	معلومات الشركة محمية من الوصول غير المصرح به.
		8	إعدادات نظام الشركة محمية من الوصول غير المصرح به.
		9	يتم مشاركة معلومات الشركة بين الأطراف المصرح لها.
السلامة	9	10	محتوى معلومات الشركة المخزنة دقيقة.
		11	محتوى معلومات الشركة المنقولة مطابقة للمعلومات الأصلية.
		12	معلومات الشركة محمية ضد التعديل غير المصرح به.
		13	إعدادات نظام الشركة محمية ضد التعديل غير المصرح به.
		14	يوفر نظام الشركة إمكانية التعرف على أي تعديلات حدثت للمعلومات.
		15	نظام الشركة يحمي المستخدمين من هجمات انتحال الهوية.
		16	يوفر نظام الشركة إمكانية التعرف على أي إتلاف حدث للمعلومات.
		17	معلومات الشركة محمية من الإتلاف غير المصرح به.
		18	أجهزة النظام ووسائط التخزين بالشركة محمية من الإتلاف.

http://doi.org/10.59222/ustjmhs.1.1.1

جدول (2): يتبع

الأبعاد	عدد الفقرات	م	الفقرات
			تقيس الفقرات الآتية مستوى أمن المعلومات في قطاع الاتصالات.
التوافر	10	19	تطبيقات نظم معلومات الشركة متاحة للمستخدمين المخولين.
		20	الموقع الخاص بالشركة متاح للمستخدمين دون انقطاع.
		21	الخدمات التي تقدمها أنظمة الشركة متاحة للمستخدمين طوال الوقت دون أي انقطاع.
		22	خوادم الشركة متاحة للمستخدمين المخولين باستمرار.
		23	النظام يُمكن المخولين من الوصول إلى المعلومات عند الطلب.
		24	توفر الشركة طاقة احتياطية للاستخدام عند انقطاع التيار.
		25	توفر الشركة موقع بديل لتشغيل نظم المعلومات في حال حدوث كوارث.
		26	سرعة الاستجابة لحوادث الأمن واستئناف العمليات.
		27	إمكانية استرداد بيانات وأنظمة الشركة بسرعة.
		28	نظام الشركة قادر على تلبية احتياجات جميع المستخدمين.

اختبار صدق المحتوى:

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

اختبار الثبات:

تم استخدام ألفا كرونباخ لاختبار الاتساق الداخلي، وتتراوح قيمة معامل ألفا كرونباخ بين (0) و (1)، وعندما تكون قيمة ألفا كرونباخ قريبة من الـ (1) يكون معامل الثبات عاليا ويقلل من تأثير خطأ القياس على درجات الاختبار (Streiner, Norman, & Cairney, 2015, 9)، ويجب أن تكون قيمة معامل ألفا كرونباخ للبُعد بين (0.70 – 0.95)، فإذا كانت أكبر من (0.95)، فتكون الفقرات متشابهة، وتؤثر على مصداقية البيانات، وتؤدي الى زيادة خطأ القياس (Hair, Hult, Ringle, & Sarstedt, 2017, 136)، ويظهر الجدول (3) نتائج اختبار ألفا كرونباخ.

جدول (3): اختبار الثبات

الأبعاد	معامل ألفا كرونباخ	عدد الفقرات
السرية	0.906	9
السلامة	0.921	9
التوافر	0.938	10

يوضح الجدول (3) أن ثبات الأبعاد تراوحت بين (0.906) للسرية كحد أدنى و(0.938) للتوافر كحد أعلى؛ أي أن مؤشرات ألفا كرونباخ للأبعاد عالية، وبالتالي، تتمتع جميع الأبعاد بدرجة عالية من الثبات، وهذا يشير إلى أن هناك اتساقا داخليا عاليا بين فقرات كل بُعد.

الأساليب الإحصائية المستخدمة:

تم استخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS) الإصدار v.25 في التحليل الوصفي، وهو الذي يشمل كل من التكرارات، والنسب المئوية، والمتوسط الحسابي، والانحراف المعياري لجميع متغيرات الدراسة.

http://doi.org/10.59222/ustjmhs.1.1.1

نتائج الدراسة ومناقشتها:

تم إجراء التحليل الوصفي؛ بهدف تحديد مستوى أمن المعلومات (السرية، والسلامة، والتوافر) في قطاع الاتصالات باليمن، وقد تم حساب المتوسط الحسابي، والانحراف المعياري، والحد الأقصى، والحد الأدنى، والنسبة المئوية، والرتبة على مستوى الفقرات والأبعاد، ويوضح الجدول (4) كيفية تفسير نتائج التحليل الوصفي لـ (218) استجابة صالحة للتحليل وفقا لمقياس ليكرت السباعي.

جدول (4): تفسير قيم المتوسط الحسابي والنسب

الوزن النسبي	تقدير المتوسط	النسبة	التقدير اللفظي	المستوى
1	1.85 - 1.00	أقل من 26 %	لا أوافق بشدة	منخفض جدا
2	2.71 - 1.86	من 26 % وأقل من 39 %		منخفض
3	3.57 - 2.72	من 39 % وأقل من 51 %		منخفض إلى حدٍ ما
4	4.43 - 3.58	من 51% وأقل من 63 %		متوسطة
5	5.29 - 4.44	من 63 % وأقل من 75 %		مرتفع إلى حدٍ ما
6	6.13 - 5.30	من 75 % وأقل من 87 %		مرتفع
7	7.00 - 6.14	من 87% إلى 100 %	أوافق بشدة	مرتفع جدا

وتعبر قيمة الانحراف المعياري عن مدى تشتت إجابة أفراد العينة حول المتوسط الحسابي، فإذا اقتربت قيمة الانحراف المعياري من (0) فهذا يدل على وجود تشتت صغير جدا، وكلما زادت قيمة الانحراف المعياري حتى قيمة (4) وسط المقياس فيدل هذا على وجود تشتت كبير في إجابة أفراد العينة عن المتوسط الحسابي، كما يعبر الحد الأدنى (1.00) والحد الأعلى (7.00) عن المستويات الدنيا والعليا في مقياس ليكرت السباعي المستخدم في الدراسة الحالية، وتُبين الجداول (5، 6، 7، 8) نتائج التحليل على مستوى أبعاد وفقرات أمن المعلومات.

أولا: مستوى أمن المعلومات في قطاع الاتصالات باليمن:

من أجل تحقيق هدف الدراسة الرئيس المتمثل في تحديد مستوى أمن المعلومات: (السرية، والسلامة، والتوافر) في قطاع الاتصالات باليمن، تم إجراء التحليل الوصفي الموضح في الجدول (5).

جدول (5): مستوى أمن المعلومات

البُعد	الرتبة	الدنيا	العليا	المتوسط	الانحراف المعياري	النسبة	المستوى
السرية	1	5.87	6.07	5.94	0.77	% 84.86	مرتفع
السلامة	2	5.60	5.85	5.72	0.92	% 81.80	مرتفع
التوافر	3	5.53	5.80	5.66	1.01	% 80.90	مرتفع
متوسط أمن المعلومات		5.67	5.91	5.77	0.90	% 82.52	مرتفع

تشير النتائج في الجدول (5) إلى أن مستوى أمن المعلومات في قطاع الاتصالات مرتفع، بمتوسط حسابي (5.77)، وانحراف معياري (0.90)، ونسبة مئوية (82.52 %). وكما أشارت النتائج إلى أن مستوى السرية في قطاع الاتصالات مرتفع، بمتوسط حسابي (5.94)، وانحراف معياري (0.77)، ونسبة مئوية (84.86 %)، وجاء بُعد السرية في المرتبة الأولى، بينما جاء بُعد التوافر في المرتبة الأخيرة بمستوى مرتفع، وبمتوسط حسابي (5.66)، وانحراف معياري (1.01)، ونسبة مئوية (80.90 %).

ويلاحظ أن أقل انحراف معياري على مستوى جميع الأبعاد كان (0.77) لبُعد السرية، وهذا يدل على وجود تشتت منخفض بين إجابات المستجيبين، ونجد أن أعلى انحراف معياري على مستوى جميع الأبعاد كان (1.01) لبُعد التوافر، ويدل هذا على وجود تشتت أعلى من السابق بين إجابات المستجيبين.

http://doi.org/10.59222/ustjmhs.1.1.1

وتتفق النتائج -التي يشير إليها الجدول (5) في أن مستوى أمن المعلومات في قطاع الاتصالات باليمن مرتفع بشكل عام- إلى حد ما مع دراسة Chang وLin (2007) التي توصلت إلى أن تنفيذ تدابير إدارة أمن المعلومات مرتفع، وكذلك تتفق مع دراسة .Al-ghananeem et al (2014) التي أشارت إلى أن مستوى معايير غايات ضمان أمن المعلومات عالية.

كذلك أظهرت النتائج في الجدول (5) أن مستوى سرية المعلومات في قطاع الاتصالات باليمن مرتفع، وقد جاء بُعد السرية في المرتبة الأولى، وهذه النتيجة تتفق مع دراسة Chang وLin (2007) التي وجدت أن مستوى السرية مرتفع، وتحتل المرتبة الأول، وأيضا تتفق إلى حد ما مع دراستي Chang وWang (2011)، و.Mohammad et al (2012) التي توصلتا إلى أن مستوى السرية مرتفع، غير أن ترتيبها كان ثانيا، وكذلك تتفق مع نتائج دراسة .Al-ghananeem et al (2014) التي أشارت إلى أن مستوى سرية البيانات كان مرتفعا، غير أن ترتيبها جاء ثالثا.

وأظهرت النتائج في الجدول (5) أن مستوى سلامة المعلومات في قطاع الاتصالات باليمن مرتفع، وقد جاء بُعد السلامة في المرتبة الثانية. وتتفق هذه النتيجة مع دراسات Chang وWang (2011) ، .Mohammad et al (2012)، و.Al-ghananeem et al (2014) التي أشارت إلى أن مستوى سلامة المعلومات مرتفع، غير أنها جاءت في المرتبة الأولى، كما تتفق أيضا مع نتائج دراسة Chang وLin (2007) التي أشارت إلى أن مستوى سلامة المعلومات كان مرتفعا وجاءت في المرتبة الثالثة.

وأشارت النتائج في الجدول (5) إلى أن مستوى توافر المعلومات في قطاع الاتصالات باليمن مرتفع، وجاء بُعد التوافر في المرتبة الثالثة، وتتفق هذه النتيجة مع دراستي .Mohammad et al (2012)، وChang وWang (2011) التي ذكرتا أن مستوى توافر المعلومات مرتفع إلى حد ما وجاءت في المرتبة الثالثة، وكذلك تتفق مع دراستي Chang وLin (2007) و.Al-ghananeem et al (2014) التي أشارت إلى أن مستوى توافر المعلومات كان مرتفعا، إلا أنها جاءت في المرتبة الثانية.

ويتضح من النتائج أن مستوى سرية المعلومات أعلى من مستوى سلامة المعلومات وتوافرها، وهذا يدل على أن سرية المعلومات تلقى اهتماما أكبر في قطاع الاتصالات باليمن مقارنة بسلامة المعلومات وتوافرها؛ وقد يرجع ذلك إلى حساسية معلومات الشركة وخصوصية بيانات العملاء، وتؤكد دراسة Deloitte (2014، 16-17) على أن سرية المعلومات في قطاع الاتصالات تُعد قضية جوهرية تؤثر في سمعة المنظمة، وتثير قلق العملاء المتعلقة بالخصوصية، وبالتالي فقدان الثقة؛ نظرا لاستخدامها على نطاق واسع في التواصل وتخزين كميات كبيرة من البيانات الحساسة، وأكد تقرير McAfee Enterprise (2016، 55) تعرض قطاع الاتصالات في أوروبا لخسائر ناتجة عن اختراق بيانات TalkTalk (هجمات تستهدف سرية البيانات) الذي أدى إلى تحول أكثر من (100,000) عميل إلى مشغلين آخرين.

ويلاحظ أن هناك اتفاقا -إلى حد كبير- بين نتائج تلك الدراسات والدراسة الحالية فيما يتعلق بمستوى السرية والسلامة والتوافر، وأيضًا هناك اختلاف واتفاق بينهما فيما يتعلق بالرتبة، وقد يرجع اختلاف رتبة السرية والسلامة والتوافر إلى اختلاف البيئة أو اختلاف القطاع الذي أجريت فيه الدراسة، فبعض القطاعات تولى اهتماما أكثر بسرية المعلومات، وبعضها يهتم أكثر بسلامة المعلومات، وأخرى تولي اهتماما أكثر بتوافر المعلومات.

ثانيا: مستوى سرية المعلومات وسلامتها وتوافرها:

1. مستوى سرية المعلومات في قطاع الاتصالات باليمن:

من أجل تحقيق الهدف الفرعي الأول للدراسة الحالية المتمثل في تحديد مستوى سرية المعلومات في قطاع الاتصالات باليمن، تم إجراء التحليل الوصفي المشار إليه في الجدول (6).

http://doi.org/10.59222/ustjmhs.1.1.1

جدول (6): مستوى سرية المعلومات

الفقرة[1]	الرتبة	الدنيا	العليا	المتوسط	الانحراف المعياري	النسبة	المستوى
السرية1	6	5.68	5.99	5.83	1.15	% 83.3	مرتفع
السرية2	7	5.54	5.90	5.72	1.34	% 81.7	مرتفع
السرية3	7	5.56	5.89	5.72	1.22	% 81.7	مرتفع
السرية4	8	5.37	5.71	5.54	1.28	% 79.1	مرتفع
السرية5	4	6.08	6.29	6.19	0.80	% 88.4	مرتفع جدا
السرية6	3	6.09	6.31	6.20	0.83	% 88.6	مرتفع جدا
السرية7	2	6.11	6.31	6.21	0.78	% 88.7	مرتفع جدا
السرية8	1	6.12	6.34	6.23	0.80	% 89.0	مرتفع جدا
السرية9	5	5.96	6.18	6.07	0.80	% 86.7	مرتفع
متوسط سرية المعلومات		5.87	6.07	5.94	0.77	% 84.86	مرتفع

أظهرت النتائج في الجدول (6) أن مستوى السرية8 (إعدادات نظام الشركة محمية من الوصول غير المصرح به) مرتفع جدا، بمتوسط حسابي (6.23)، وانحراف معياري (0.80)، ونسبة مئوية (89 %)، وجاءت في المرتبة الأولى، وأظهرت النتائج أن مستوى السرية7 (معلومات الشركة محمية من الوصول غير المصرح به) مرتفع جدا، وجاءت في المرتبة الثانية بنسبة (88.7 %)، وتشير هذه النتيجة إلى فاعلية المصادقة والتحكم بالوصول المنطقي والمادي إلى موارد نظم المعلومات في قطاع الاتصالات باليمن؛ كون المصادقة والتحكم بالوصول يدعمان عمليات الشركة الحيوية، ويسمحان بالوصول المصرح به، ويرفضان الوصول غير المصرح به، ويحافظان على سرية المعلومات من الكشف، كما يبدأ الأمن بتحديد الهوية، ثم التحقق من الهوية، ثم التحكم بالوصول إلى الموارد، وهذه النتيجة تختلف قليلا عن دراسة Chang وWang (2011) التي توصلت إلى أن مستوى حماية بيانات الشركة من الوصول غير المصرح به مرتفع إلى حد ما وبنسبة (72 %)، وأيضا تختلف عن دراسة .Mohammad et al (2012) التي وجدت أن مستوى استخدام الجدران النارية في حماية شبكة الجامعة من المتطفلين مرتفع إلى حد ما بنسبة (65 %)، وتختلف عن دراسة Khanyako وMaiga (2013، 6) التي أظهرت أن مستوى إمكانيّة الوصول إلى المعلومات المصرفية الإلكترونية منخفض إلى حد ما وبنسبة (50.2 %)، وقد يرجع الاختلاف بين الدراسة الحالية والدراسات السابقة إلى اختلاف القطاع أو اختلاف البيئة التي أجريت فيها الدراسة، فأهمية السرية تختلف من قطاع إلى آخر.

وكما أشارت النتائج في الجدول (6) إلى أن مستوى السرية4 (حسابات المستخدمين على صفحات الويب الخاصة بالشركة محمية من الكشف) مرتفع، لكنه جاء في المرتبة الأخيرة، وبمتوسط حسابي (5.54)، وانحراف معياري (1.28)، ونسبة مئوية (79.1 %)، وقد يرجع ظهور السرية4 في المرتبة الأخيرة إلى وجود قصور محدود في تنفيذ الضوابط الإدارية كالتوعية والتدريب في مجال أمن المعلومات، وتطبيق سياسة أمن المعلومات، وإجراءات التدقيق، أو أن هناك قصورا محدودا في تنفيذ الضوابط التقنية من قبل الإدارة المعنية في حماية صفحات المستخدمين على الويب، وهذه النتيجة تتفق إلى حد ما مع دراسة .Mohammad et al (2012) التي توصلت إلى أن مستوى حماية صفحات المستخدمين على الويب مرتفع جدا وبنسبة (87.5 %).

2. مستوى سلامة المعلومات في قطاع الاتصالات باليمن:

من أجل تحقيق الهدف الفرعي الثاني للدراسة الحالية المتمثل في تحديد مستوى سلامة المعلومات في قطاع الاتصالات باليمن، تم إجراء التحليل الوصفي المشار إليه في الجدول (7).

[1] محتوى الفقرات من السرية1 إلى السرية9 مذكورة في الجدول (2) ضمن بُعد السرية.

http://doi.org/10.59222/ustjmhs.1.1.1

جدول (7): مستوى سلامة المعلومات

الفقرة[1]	الرتبة	الدنيا	العليا	المتوسط	الانحراف المعياري	النسبة	المستوى
السلامة10	4	5.62	5.93	5.77	1.17	% 82.4	مرتفع
السلامة11	2	5.73	6.03	5.88	1.12	% 84.0	مرتفع
السلامة12	1	5.74	6.04	5.89	1.12	% 84.1	مرتفع
السلامة13	3	5.71	6.02	5.86	1.14	% 83.7	مرتفع
السلامة14	6	5.56	5.87	5.72	1.15	% 81.7	مرتفع
السلامة15	7	5.45	5.77	5.61	1.20	% 80.1	مرتفع
السلامة16	9	5.31	5.67	5.49	1.36	% 78.4	مرتفع
السلامة17	5	5.62	5.89	5.76	1.01	% 82.3	مرتفع
السلامة18	8	5.37	5.73	5.55	1.33	% 79.3	مرتفع
متوسط سلامة المعلومات		5.60	5.85	5.72	0.92	% 81.8	مرتفع

يتضح من الجدول (7) أن مستوى السلامة12 (معلومات الشركة محمية ضد التعديل غير المصرح به) مرتفع، بمتوسط حسابي (5.89)، وانحراف معياري (1.12)، ونسبة مئوية (84.1 %)، وجاءت في المرتبة الأولى، وهذه النتيجة تتفق إلى حد ما مع دراسة Chang وLin (2007) التي توصلت إلى أن مستوى حماية المعلومات من التغيير غير المصرح به مرتفع، وبنسبة (74.86 %)، وتؤكد هذه النتيجة على أهمية حماية بيانات الشركة وحماية الأجهزة والبرامج المستخدمة في تبادل البيانات، ومعالجتها، وتخزينها من التعديل غير المصرح به؛ كون تعديل البيانات يؤثر في سمعة الشركة، والعمليات، والتقارير المالية، والربحية، كما أن الحفاظ على سلامة المعلومات يحقق الثقة في المعلومة لدى المتعاملين بأنها كاملة في محتواها، وصحيحة في مضمونها، وجرت معالجتها بالطرق الصحيحة، وعندما يتعلق الأمر بتعديل بيانات مالية تصبح سلامة البيانات في أنظمة المعلومات بالغة الأهمية، وقد كشف تقرير McAfee Enterprise (2015، 35) عن استخدام برنامج ضار (يعمل على تعديل البيانات) في مهاجمة المصارف، مثل البرنامج الضار Carbanak الذي تمكن من اختراق (100) مصرف.

وأظهرت النتائج في الجدول (7) أن مستوى السلامة16 (يوفر نظام الشركة إمكانية التعرف على أي إتلاف حدث للمعلومات) مرتفع، لكنه جاء في المرتبة الأخيرة، وبمتوسط حسابي (5.49)، وانحراف معياري (1.36)، ونسبة مئوية (78.4 %)، وتدل هذه النتيجة على أن قطاع الاتصالات في اليمن يولي اهتماما أقل فيما يتعلق بالرقابة على أي إتلاف حدث للمعلومات.

3. مستوى توافر المعلومات في قطاع الاتصالات باليمن:

من أجل تحقيق الهدف الفرعي الثالث للدراسة الحالية المتمثل في تحديد مستوى توافر المعلومات في قطاع الاتصالات، تم إجراء التحليل الوصفي الموضح في الجدول (8).

جدول (8): مستوى توافر المعلومات

الفقرة[2]	الرتبة	الدنيا	العليا	المتوسط	الانحراف المعياري	النسبة	المستوى
التوافر19	2	6.04	6.26	6.15	0.82	87.9%	مرتفع جدا
التوافر20	5	5.47	5.80	5.64	1.25	80.6%	مرتفع
التوافر21	6	5.40	5.75	5.57	1.34	79.6%	مرتفع
التوافر22	4	5.62	5.96	5.79	1.25	82.7%	مرتفع
التوافر23	3	5.72	6.04	5.88	1.18	84.0%	مرتفع
التوافر24	1	6.01	6.31	6.16	1.13	88.0%	مرتفع جدا

[1] محتوى الفقرات من السلامة10 إلى السلامة18 مذكورة في الجدول (2) ضمن بُعد السلامة.
[2] محتوى الفقرات من التوافر19 إلى التوافر28 مذكورة في الجدول (2) ضمن بُعد التوافر.

http://doi.org/10.59222/ustjmhs.1.1.1

جدول (8): يتبع

الفقرة[1]	الرتبة	الدنيا	العليا	المتوسط	الانحراف المعياري	النسبة	المستوى
التوافر25	10	5.01	5.43	5.22	1.56	74.6%	مرتفع إلى حدٍ ما
التوافر26	9	5.21	5.57	5.39	1.32	77.0%	مرتفع
التوافر27	8	5.22	5.57	5.40	1.31	77.1%	مرتفع
التوافر28	7	5.24	5.60	5.42	1.36	77.4%	مرتفع
متوسط توافر المعلومات		5.53	5.80	5.66	1.01	80.9%	مرتفع

يتضح من الجدول (8) أن مستوى التوافر24 (توفر الشركة طاقة احتياطية للاستخدام عند انقطاع التيار) مرتفع جدا، وبمتوسط حسابي (6.16)، وانحراف معياري (1.13)، ونسبة مئوية (88 %)، وجاءت في المرتبة الأولى، وتشير هذه النتيجة إلى أن قطاع الاتصالات في اليمن يولي اهتماما أكبر بالطاقة الاحتياطية؛ نظرا للانعدام الكلي للطاقة العمومية، والواقع يؤكد صحة ما تم التوصل إليه، وقد ذكر تقرير ISBS (2013، 18) أن شركات التكنولوجيا عانت من انقطاع الطاقة الذي أدى إلى تعطل الأعمال لعدة أيام، وتتطلب خدمة التوافر جعل الأنظمة والخدمات متاحة لمستخدميها بشكل دائم، وعدم توافر الطاقة العمومية أو الاحتياطية يعني توقف الخدمات التي تقدمها الشركة، وفقدان إيرادات، وتحول العملاء إلى مشغلين آخرين، وضمان التوافر يشمل استمرار العمليات، وإمكانية الوصول إلى البيانات، وسهولة استخدامها من قبل الأطراف المصرح لها في أي وقت، وهذه النتيجة تختلف عن دراسة Mohammad et al. (2012) التي توصلت إلى أنه يتم التعامل مع انقطاعات نظام إدارة التعلم بشكل صحيح بمستوى متوسط ونسبة (62.25 %)، وقد يعود هذا الاختلاف إلى اختلاف القطاع الذي أجريت فيه الدراسة.

وأظهرت النتائج في الجدول (8) أن مستوى التوافر25 (توفر الشركة موقع بديل لتشغيل نظم المعلومات في حال حدوث كوارث) مرتفع إلى حد ما، ولكنه جاء في المرتبة الأخيرة، وبمتوسط حسابي (5.22)، وانحراف معياري (1.56)، ونسبة مئوية (74.6 %)، وهذا يدل على أن قطاع الاتصالات يولي اهتماما أقل بتوفير موقع بديل في حال تعرض الموقع الرئيس لكوارث طبيعية وغير طبيعية، وقد يرجع ذلك إلى ضعف خطة التعافي من الكوارث، أو ضعف خطة الاستجابة للحوادث السيبرانية، أو انخفاض الوعي والإدراك بأهمية إنشاء موقع بديل، وفي حال عدم جاهزية الموقع البديل يعني توقف النظام عن العمل، وفقدان ثقة العملاء بالخدمة التي تقدمها الشركة، وتحول العملاء إلى مشغلين آخرين، وهذه النتيجة تتفق مع دراسة Chang وLing (2007) التي أشارت إلى أن الشركة تعمل على حماية نظام المعلومات من الانهيار أو تعطل خدمة المعلومات بمستوى مرتفع إلى حدٍ ما ونسبة (71.86 %).

الاستنتاجات:

بناء على نتائج التحليل الوصفي ومناقشتها تم التوصل إلى الاستنتاجات الآتية:

1) هناك اهتمام واسع بأمن المعلومات في قطاع الاتصالات باليمن، وفي مقدمة اهتمامات قطاع الاتصالات سرية المعلومات، يليها سلامة المعلومات والأنظمة، ثم توافر الأنظمة والمعلومات والخدمات.
2) تلقى سرية المعلومات في قطاع الاتصالات باليمن اهتماما كبيرا بما في ذلك التحكم بالوصول المنطقي والمادي، وآليات التحقق من الهوية، والتشفير.
3) أيضا هناك اهتمام بسلامة المعلومات في قطاع الاتصالات باليمن، ويركز قطاع الاتصالات أكثر على حماية البيانات المخزنة أو المنقولة ضد التعديل غير المصرح به.
4) يلاحظ أن ارتفاع مستوى التوافر في قطاع الاتصالات باليمن يعود إلى الطاقة الاحتياطية المتاحة، والتطبيقات المتاحة للمستخدمين المخولين، وإمكانية الوصول إلى الخدمة عند الطلب.

[1] محتوى الفقرات من التوافر19 إلى التوافر28 مذكورة في الجدول (2) ضمن بُعد التوافر.

http://doi.org/10.59222/ustjmhs.1.1.1

التوصيات:

توصي الدراسة الحالية قطاع الاتصالات باليمن بالآتي:

1) **تعزيز أمن المعلومات للحفاظ على سرية المعلومات، وسلامة المعلومات والأنظمة، وتوافر الأنظمة والمعلومات والخدمات؛ وإيلاء كل من السرية، والتوافر، والسلامة مزيدا من الاهتمام؛ كونهما الأكثر أهمية في قطاع الاتصالات، التي تؤدي إلى زيادة الثقة ورفع مستوى أمن المعلومات في قطاع الاتصالات عينة الدراسة.**
2) **دعم إجراءات حماية المعلومات الحساسة في الشركة، وحماية الخصوصية الشخصية للعملاء، وتقييد عمليات الوصول المصرح به، وحماية حسابات المستخدمين على صفحات الويب.**
3) **تعزيز إجراءات حماية المعلومات والأنظمة والخدمات من التعديل أو الإتلاف غير المصرح به التي تستهدف سلامة وتكامل المعلومات والأنظمة، وتعزيز إجراءات التعرف على أي إتلاف أو تعديل حدث للمعلومات وحماية أجهزة النظام ووسائط التخزين من الإتلاف.**
4) **دعم أنشطة الوصول المصرح به إلى أنظمة المعلومات والخدمات عند الطلب وتعزيز الثقة في أنظمة المعلومات من خلال توفير موقع بديل لتشغيل النظام، وسرعة الاستجابة للحوادث الأمنية.**

المقترحات:

1) **تم إجراء هذه الدراسة على قطاع الاتصالات فقط، وقد تكون النتائج غير قابلة للتعميم على بقية القطاعات، لذلك ينبغي توسيع نطاق البحث؛ ليشمل أنواع مختلفة من القطاعات، مثل: إجراء دراسات مماثلة في البنوك، والمستشفيات، والجامعات.**
2) **إجراء مزيد من الأبحاث لاستكشاف العوامل التي تؤثر في أمن المعلومات: (السرية، والسلامة، والتوافر) سلبا وإيجابا والتي قد تساعد في تعزيز أمن المعلومات في مختلف القطاعات.**

المراجع:

البشيري، منصور (2021، **يناير** 11)، ***آثار الصراع على قطاع الاتصالات في اليمن***، **استرجع من موقع مركز صنعاء للدراسات الاستراتيجية:** https://bit.ly/3tJaGaD

حجر، عبدالملك إسماعيل (2014)، ***نظم المعلومات المحاسبية*** **(الطبعة الرابعة)، صنعاء، اليمن: الأمين للنشر والتوزيع.**

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

سبأ نت (2014)، ***المؤتمر الأول لأمن المعلومات- صنعاء***، **استرجع من** https://bit.ly/3EkbVC8

الشوكاني، غمدان (2016، **مايو** 11)، ***أكثر من 37 مليار ريال خسائر مؤسسة الاتصالات منذ بدء العدوان***، **استرجع من موقع وكالة الأنباء اليمنية سبأ:** https://bit.ly/3VbISHK

عدن الغد (2014)، ***خلل بشبكة (MTN) يوقف حركة الاتصالات بعدن***، **استرجع بتاريخ يونيو** 6، 2017، **من** https://adengad.net/public/posts/103375

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

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

يحيى، عماد (2012)، **الهجمات الإلكترونية كأكبر المخاطر التي تهدد قطاع الأعمال، استرجع بتاريخ نوفمبر** 19، 2015، **من** https://bit.ly/3OhZ08d

http://doi.org/10.59222/ustjmhs.1.1.1

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-ghananeem, K. M., Al-taee, M. A., & Jida, B. K. (2014). The impact of the goals of information security standards to ensure information security. *Journal of Management Research, 6*(2), 74-101.

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

Berisha, A., & Tawfik, M. (2016). *Applying ISO/IEC 27001 in the telecommunications industry, PECB*. Retrieved Sep 12, 2022, from https://bit.ly/3TK0Boo

Bernews (December 2, 2015). *EY global information survey: Cyber attacks*. Retrieved February 08, 2018, from https://bit.ly/3V8G2mz

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

Centre for Cybersecurity (2022). T*hreat assessment: The cyber threat against the telecom sector*. Retrieved Sep 9, 2022, from https://bit.ly/3At1tqA

CERT-AU & Australian Cyber Security Centre (ACSC) (2015). *Cyber security survey: Major Australian businesses*. Australia: CERT-AU & ACSC.

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

Chang, S. E., & Lin, C. S. (2007). Exploring organizational culture for information security management. *Industrial Management & Data Systems, 107*(3), 1-34.

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

Deloitte. (2006). *Protecting the Digital Assets: The 2006 Technology, Media & Telecommunications Security Survey*. London, United Kingdom: Deloitte Touche Tohmatsu Limited (DTTL).

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

Donaldson, S., Siegel, S., Williams, C. K., & Aslam, A. (2015). *Enterprise cybersecurity: How to build a successful cyberdefense program against advanced threats*. New York: Springer Science+Business Media Finance, Inc.

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

http://doi.org/10.59222/ustjmhs.1.1.1

FISMA. (2016). *Annual report to congress: Federal information security modernization act*. Washington, D.C.: Office of Management and Budget.

Government Accountability Office (GAO). (2016a). *Information security: FDIC implemented controls over financial systems, but further improvements are needed* (GAO-16-605). Washington: GAO.

Government Accountability Office (GAO). (2016b). *Information security: Agencies need to improve controls over selected high-impact systems* (GAO-16-501). Washington: GAO.

Hair, J. F., Hult, T. M., Ringle, C. M., & Sarstedt, M. (2017). *A Primer on Partial Least Squares Structural Equation Modeling* (PLS-SEM) (2nd ed.). Thousand Oakes, CA: Sage.

Hulme, G. V. (2015). *Survey says enterprises are stepping up their security game*. Retrieved from CSO on line: https://bit.ly/3Epcp9Sl

Information Systems Audit and Control Association (ISACA) (2012). *ISACA® Glossary of Terms English-Arabic*. Schaumburg, IL: ISACA.

International Telecommunication Union (ITU) & ABIresearch (2015). *Global Cybersecurity Index & Cyberwellness Profiles*. Geneva: ITU. Retrieved May 29, 2015, from https://bit.ly/3tKe44W

International Telecommunication Union (ITU) (2014). *Understanding cybercrime: Phenomena, challenges and legal response*. Switzerland, Geneva: Telecommunication Development Sector.

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

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

International Telecommunication Union (ITU). (2021). *Global cybersecurity index (GCI)*. Switzerland Geneva: Telecommunication Development Sector and ABI research.

ISBS (2013). *Information security breaches survey: Technical report*. London: Survey conducted by PwC in association with Infosecurity Europe.

ISBS (2014). *Information security breaches survey: Technical report*. London: Survey conducted by PwC in association with Infosecurity Europe.

ISO/IEC JTC 1 (2011). I*nformation technology — Security techniques — Information security risk management* (ISO/IEC 27005) (2nd ed.). Washington, D.C.: ISO/IEC JTC 1.

ISO/IEC JTC 1 (2018). *Information technology — Security techniques — Information security management systems — Overview and vocabulary* (ISO/IEC 27000) (5th ed.). Washington, D.C.: ISO/IEC JTC 1.

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

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

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

Khanyako, E., & Maiga, G. (2013). *An information security model for eGovernment services adoption in Uganda*. Paper presented at the IIMC International Information Management Corporation, 9-11 October, Dublin, Ireland.

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

Lehto, M., & Neittaanmäki, P. (2022). *Cyber security: Critical infrastructure protection* (Volume 56). Switzerland AG, Springer.

McAfee Enterprise (2015). *McAfee labs 2016 threats predictions report*. Retrieved from https://bit.ly/3gkSnW0

McAfee Enterprise (2016). *McAfee labs 2017 threats predictions report*. Retrieved from https://bit.ly/3Eez9Jy

Mohammad, S., Awadhi, A. A., Kananah, A., & Job, M. A. (2012). Security Management Policy of LMS in AOU Bahrain Branch. *International Journal of Information and Communication Technology Research, 2*(6), 484-490.

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

Neogy, D. (2014). Evaluation of efficiency of accounting information systems: A study on mobile telecommunication companies in Bangladesh. *Global Disclosure of Economics and Business, 3*(1), 40-55.

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

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

http://doi.org/10.59222/ustjmhs.1.1.1

Peltier, T. R. (2014). *Information security fundamentals* (2nd ed.). Boca Raton, Florida: Taylor & Francis Group.

PricewaterhouseCoopers (PwC) & Infosecurity (2015). *Information security breaches survey: technical report*. London: PwC.

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

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

Richardson, R. (2010). *2010 / 2011 computer crime and security survey*. In the 15th Computer Security Institute (CSI) annual conference. New York: CSI.

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

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

Streiner, D. L., Norman, G. R., & Cairney, J. (2015). *Health measurement scales: A practical guide to their development and use* (5th ed.). New York: Oxford University Press.

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

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

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

Arabic References in Roman Scripts:

Aden Alghad (2014). *Khalal bishabaka (MTN) yuqif harakat aliatisalat bi Aden.* Asturjie bitarikh Yunyu 6, 2017, min https://bit.ly/3Gv2Nxg

Al-Bashiri, Mansour (2021, Ynayir 11). *Athar alsirae ealaa qitae alaitisalat fi Alyamin*. Aistarjie min mawqie Markaz Sana'a Lidirasat Alastiratijiati: https://sanaacenter.org/ar/publications-all/main-publications-ar/12723

Al-Qahtani, Theeb bin Ayedh (2015). *Amn almaelumat* (Taba'a 1), Alrayad, Alsueudiatu: Maktabat Almalik Fahd Alwataniati.

Al-Rubaidi, Muhammad Ali (2010). Himayatu almaelumati almuhasabiati fi zal makhatiru altiknulujya laleamaliaati almasrifiati al'iilikturuniati: Dirasati midaniati fi albunuka aleamilati fi alimin, *Mijalatun Kiliyata Altijarati Walaiqtisad, 33*, 1-45.

Al-Shawkani, Ghamdan (2016, Mayu 11). *Akthar min 37 milyar rial khasayir Muasasat Alaitisalat mundh bad' aleudwani*. Aistarjie min mawqie Wakalat Al'anba' Alyamaniat Saba'a: https://www.saba.ye/ar/news427488.htm

Fadel, Abdul Karim Muhammad Yahya (2018). *Taqyimu makhatiri 'amin nazumi almaelumati almuhasabiati almuhawsabati lidaa albunuka altijariati fi Alyaman: dirasatan tatbiqiatan* (Utaruhatan dukturah), Jamieat Dimashqa, Suria.

Hajar, Abdul Malik Ismail (2014). *Nuzum almaelumat almuhasabia* (Taba'a 4), Sana'a, Alyamanu: Al'amin Lilnashr Waltawziei.

Saba Net (2014). *Almutamaru al'uwla li'amn almaelumati – Sana'a*. Aistarjie min https://yemennic.info/conferences/activ_details.php?ID=69967

Yahya, Emad (2012). *Alhajamati al'iiliktiruniati ka'akbari almakhatiri alti tahadidu qitaei al'aemali*. Astarjie bitarikh Nufimbir 19, 2015, min https://bit.ly/3Ojqn1A

http://doi.org/10.59222/ustjmhs.1.1.1