

تحليل الأمن السيبراني في نظم المعلومات المحاسبية وتأثيره على حماية البيانات المالية الحساسة للشركات الصناعية الليبية: دراسة استطلاعية من وجهة نظر الموظفين بالإدارة المالية بمصنع أسمنت المرقب

خالد بشير محمد أحمد

كلية الاقتصاد، صرمان، جامعة صبراتة، ليبيا
KHALED.AHMED@SABU.EDU.LY

مراد أمحمد أبوشعالة

المعهد العالي للعلوم والتقنية، الرحيبات، ليبيا
MURADAA221@GMAIL.COM

المستخلص

هدفت هذه الدراسة إلى التعرف على تحليل الأمن السيبراني في نظم المعلومات المحاسبية وتأثيره على حماية البيانات المالية الحساسة للشركات الصناعية الليبية، وذلك من خلال التعرف على مفهوم تحليل الامن السيبراني، ولتحقيق هذه الأهداف تم اتباع المنهج الوصفي التحليلي وذلك من خلال الاطلاع على الكتب والمجلات والرسائل العلمية وما يتوفر على الإنترنت بالشكل الذي يخدم أغراض الدراسة، وقد تم الاعتماد على المنهج الوصفي التحليلي لتحليل البيانات واستخلاص النتائج باستخدام البرنامج التحليلي الإحصائي SPSS في الدراسة، كما استخدم الباحثان الاستبانة لتجميع البيانات اللازمة لإجراء هذه الدراسة حيث تم توزيع (25) استبانة، استرجع منها (22) استبانة بنسبة 88%، وبعد المراجعة تبين أنها صالحة للمعالجة الإحصائية، يتمثل مجتمع الدراسة (مصنع أسمنت المرقب) في جميع موظفين الإدارة المالية، فقد تم حصر ذلك فقط واستخدام مسح شامل لكافة العينة، ثم توصلت الدراسة إلى مجموعة من النتائج أهمها: يؤثر تحليل الأمن السيبراني على حماية البيانات المالية الحساسة في نظم المعلومات المحاسبية كذلك تؤثر سياسات التحكم في الوصول على أمن البيانات المالية الحساسة وأنه لا يتم تحديد وقياس فعالية استراتيجيات استجابة الحوادث عند حدوث خرق بيانات لدى مصنع أسمنت المرقب.

وقد خلصت الدراسة إلى مجموعة من التوصيات أهمها: يجب أن يتم تحديد وقياس فعالية استراتيجيات استجابة الحوادث عند حدوث خرق بيانات وتنظيم ورش عمل وبرامج تدريبية للموظفين حول أهمية تحليل الأمن

السيبراني وتأثيره وإجراء تقييم شامل للمخاطر السيبرانية التي تواجه نظم المعلومات المحاسبية في الشركات الصناعية. يُمكن استخدام أدوات تحليل المخاطر لتحديد الثغرات المحتملة.
الكلمات الافتتاحية: تحليل الأمن السيبراني، نظم المعلومات المحاسبية، البيانات المالية، الشركات الصناعية.

Cybersecurity analysis in accounting information systems and its impact on the protection of sensitive financial data of Libyan industrial companies: A survey study from the perspective of employees in the financial department of the Marqab Cement Factory

Khaled Bashir Mohammed Ahmed

Faculty of Economics, Sorman, University of Sabratha, Libya
KHALED.AHMED@SABU.EDU.LY

Murad Amhamed Abu-Shaala

Higher Institute of Science and Technology, Al-Rahibat, Libya
MURADAA221@GMAIL.COM

Abstract

The aim of this study was to analyze cybersecurity in accounting information systems and its impact on protecting sensitive financial data of Libyan industrial companies. This was achieved by understanding the concept of cybersecurity analysis. To achieve these goals, the descriptive analytical method was adopted by reviewing books, journals, research papers, and available online resources that serve the study's purposes. The descriptive analytical approach was used to analyze the data and extract results using the SPSS statistical analysis program. The researchers used a questionnaire to gather the necessary data for this study, distributing 25 questionnaires, with 22 returned, representing an 88% response rate. After review, the questionnaires were found to be valid for statistical processing. The study population consisted of all employees of the financial management department at the

Al-Marqab Cement Factory, where a comprehensive survey of the entire sample was conducted.

The study reached several conclusions, the most important being that cybersecurity analysis affects the protection of sensitive financial data in accounting information systems, and access control policies impact the security of sensitive financial data. Additionally, the effectiveness of incident response strategies is not determined or measured when a data breach occurs at Al-Marqab Cement Factory.

The study concluded with several recommendations, the most important of which include: the need to define and measure the effectiveness of incident response strategies during data breaches, organizing workshops and training programs for employees on the importance of cybersecurity analysis and its impact, and conducting a comprehensive assessment of the cyber risks facing accounting information systems in industrial companies. Risk analysis tools can be used to identify potential vulnerabilities.

Keywords: Cybersecurity Analysis, Accounting Information Systems, Financial Data, Industrial Companies.

المقدمة

في عصر التكنولوجيا الحديثة واندماجها العميق في جميع مجالات الأعمال، أصبحت نظم المعلومات المحاسبية أحد الأعمدة الأساسية لكل المؤسسات. تعمل هذه النظم على إدارة البيانات المالية وتسهيل العمليات المالية والمحاسبية. ومع تزايد اعتماد المؤسسات على هذه الأنظمة، زادت المخاطر السيبرانية التي تهددها، لذا يُعد فهم الأمن السيبراني وتحليله جزءاً أساسياً لضمان سلامة البيانات المالية الحساسة.

الأمن السيبراني تشمل مجموعة من الاستراتيجيات والتقنيات التي تهدف إلى حماية المعلومات من الهجمات الإلكترونية والاحتمالات والمخاطر الأخرى، إن تحليل الأمن السيبراني في نظم المعلومات المحاسبية يركز على تحديد نقاط الضعف في النظام والتعرف على التهديدات المحتملة، مما يساهم في تعزيز الأمن والحد من الخسائر المالية والمعنوية.

تزايد التحديات التي تواجه نظم المعلومات المحاسبية بسبب تطور أساليب الهجوم وابتكار تقنيات جديدة. ولذلك، تعتبر معالجة هذه القضايا أمرًا حيويًا. يتطلب الأمر تبني استراتيجيات دفاعية قوية، مثل تشفير البيانات، وتطبيق ضوابط وصول صارمة، وتوفير التدريب المستمر للموظفين حول أفضل ممارسات الأمن. تأثير الأمن السيبراني على حماية البيانات المالية ليس فقط في منع فقدان البيانات أو الوصول غير المصرح به، ولكن أيضًا في تعزيز الثقة بين الشركات وعملائها. فالأمن السيبراني الجيد يُحسن من سمعة المؤسسة ويساهم في بناء علاقات موثوقة مع الشركاء والمستثمرين.

في النهاية، ينبغي على جميع المؤسسات إدراك أهمية تحليل الأمن السيبراني في نظم المعلومات المحاسبية. فمن خلال التركيز على هذه المرونة الأمنية، يمكن للمؤسسات حماية بياناتها المالية الحساسة وتحقيق استدامتها ونموها في بيئة أعمال تتسم بالتنافسية العالية.

مشكلة الدراسة

تعتبر مشكلة الأمن السيبراني في نظم المعلومات المحاسبية تحديًا معقدًا يتطلب اتباع استراتيجيات متعددة الأبعاد لحماية البيانات المالية الحساسة. من خلال تعزيز الوعي والتدريب للمستخدمين، وتطبيق أحدث تقنيات الأمن، يمكن للشركات تقليل المخاطر المرتبطة بالجرائم السيبرانية وضمان حماية بياناتها الحيوية. وفقًا لتقرير صادر عن "Cybersecurity Ventures"، يُتوقع أن تصل تكاليف الأضرار الناتجة عن الجرائم السيبرانية إلى 10.5 تريليون دولار سنويًا بحلول عام 2025، مما يوضح الأثر الاقتصادي الكبير لهذه المشكلة. كثير من نظم المعلومات المحاسبية تفتقر إلى تدابير الأمن المطلوبة، حيث تشير دراسة أجرتها "Gartner" إلى أن 90% من الهجمات تستغل ثغرات معروفة لم يتم تصحيحها، مما يسلب الضوء على الحاجة الملحة لتحسين الأمن السيبراني ويمكن صياغة مشكلة الدراسة في السؤال التالي:

كيف يؤثر تحليل الأمن السيبراني على حماية البيانات المالية الحساسة في نظم المعلومات المحاسبية؟

ويتفرع من التساؤل الرئيسي مجموعة من التساؤلات الفرعية التالية:

- كيف تؤثر سياسات التحكم في الوصول على أمن البيانات المالية الحساسة؟

- كيف يتم تحديد وقياس فعالية استراتيجيات استجابة الحوادث عند حدوث خرق بيانات؟

- كيف يمكن استخدام تحليل البيانات للكشف عن نقاط الضعف في نظم المعلومات المحاسبية؟

أهداف الدراسة

- الهدف الرئيسي: تحليل تأثير الأمن السيبراني على حماية البيانات المالية الحساسة في نظم المعلومات المحاسبية.

- الأهداف الفرعية:

1. تقييم مستوى الأمن في نظم المعلومات المحاسبية.
2. تحليل استراتيجيات الأمن المتبعة لحماية المعلومات.
3. دراسة تأثير الحوادث السيبرانية على الأداء المالي والمؤسسي.
4. تقديم توصيات لتحسين الأمن السيبراني في نظم المعلومات المحاسبية.

أهمية الدراسة

- الأهمية العلمية: تطوير المعرفة ويساهم الموضوع في تطوير المفاهيم والنظريات المتعلقة بكيفية حماية البيانات المالية الحساسة من التهديدات السيبرانية ويوفر إطارًا للدراسات المستقبلية التي تركز على تحسين أنظمة الأمن ومواجهة الهجمات الإلكترونية ويساعد في فهم طبيعة المخاطر المرتبطة بأنظمة المعلومات المحاسبية وبالتالي تحسين استراتيجيات الحماية.

- الأهمية العملية: يساعد في حماية المعلومات الحساسة مثل البيانات المالية، مما يضمن سلامة العمليات المحاسبية ويعزز من فعالية نظم المعلومات من خلال تقليل المخاطر وزيادة الأمن، مما يساهم في تحقيق أهداف المؤسسة ويساعد المؤسسات على الالتزام باللوائح والأنظمة المتعلقة بحماية البيانات، مما يعزز من سمعتها وثقة عملائها.

- الأهمية الاجتماعية: يساهم في حماية المعلومات الشخصية والمالية للأفراد، مما يعزز من الثقة في النظم المالية والتجارية ويلعب دورًا في توعية المجتمع حول أهمية الأمن السيبراني وكيفية حماية البيانات الشخصية ومن خلال تأمين البيانات المالية، يساهم في الاستقرار الاقتصادي ويحد من الجرائم السيبرانية التي تؤثر سلبيًا على المجتمع.

فرضيات الدراسة

تنص الفرضية الرئيسية بأنه "يؤثر تحليل الأمن السيبراني على حماية البيانات المالية الحساسة في نظم المعلومات المحاسبية".

ولكي يتم اختبار هذه الفرضية تم صياغة الفرضيات الفرعية التالية:

- تؤثر سياسات التحكم في الوصول على أمن البيانات المالية الحساسة.
- يتم تحديد وقياس فعالية استراتيجيات استجابة الحوادث عند حدوث خرق بيانات.
- يتم استخدام تحليل البيانات للكشف عن نقاط الضعف في نظم المعلومات المحاسبية.

حدود الدراسة

- أ. الحدود الموضوعية: تتركز على تحليل الأمن السيبراني في نظم المعلومات المحاسبية وتأثيره على حماية البيانات المالية الحساسة من وجهة النظر الموظفين العاملين بالإدارة المالية الشركة الأهلية للأسمنت المساهمة (مصنع أسمنت المرقب) عينة الدراسة.
- ب. الحدود المكانية: الموظفين العاملين بالإدارة المالية بمصنع أسمنت المرقب.

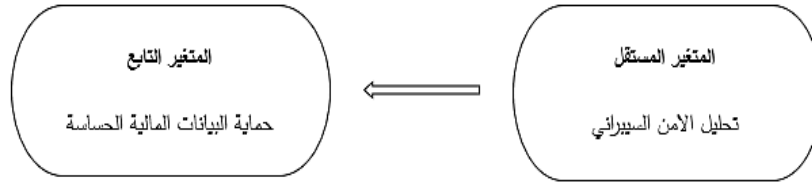
منهج الدراسة

- لتحقيق أهداف الدراسة فقد تم تقسيم منهجية البحث إلى:
 - أ. تم تكوين الجانب النظري من خلال الاطلاع على الكتب والدوريات العلمية والمنشورات المختلفة والمنهج الاستنباطي عند إعداد الدراسات الميدانية للدراسة.
 - ب. مجتمع الدراسة والعينة: يمثل مجتمع الدراسة الشركة الأهلية للأسمنت المساهمة (مصنع أسمنت المرقب).
 - ت. طرق جمع البيانات (الاستبيان): للحصول على البيانات اللازمة لإجراء الدراسة الميدانية للدراسة اعتمد الباحثان على استمارة الاستبيان كأداة رئيسية لتجميع البيانات.
 - ث. طرق تحليل البيانات (برنامج SPSS): تم استخدام أساليب الإحصاء الوصفي، واختبار توزيع التحليل بيانات الدراسة.

متغيرات الدراسة

تتمثل المتغيرات التي تتناولها الدراسة فيما يلي:

تحليل الأمن السيبراني (متغير مستقل)، حماية البيانات المالية الحساسة (متغير تابع).



مصطلحات الدراسة

يتم تعريف مصطلحات الدراسة كالتالي:

تتابع تطور مجال تقنية المعلومات وتوسعت مجالاته وتفرعاته، ونتيجة لذلك التطور توسعت تفرعات أمن المعلومات بشكل مضطرب وظهر المصطلح الحديث لمجال حماية المعلومات والفضاء الذي يحتوي كل ماله علاقة بتلك المعلومات وانتشر على نطاق واسع وهو "الأمن السيبراني" وأصبح مصطلح شاملاً يضم كل المصطلحات والتعريفات المتعلقة بالمعلومات وحمايتها في جميع الصور (رقمياً وغير رقمي) فبحسب تعريف الهيئة الوطنية لأمن السيبراني، ينص تعريف الأمن السيبراني على "حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك" (الهيئة الوطنية للأمن السيبراني، 2018)

الدراسات السابقة

1. دراسة (ايمان السيد محمد عبدالله، 2024) بعنوان، دراسة العلاقة بين تفعيل أدوات الأمن السيبراني وأنظمة محاسبة التكاليف الرقمية دراسة تطبيقية علي شركات القطاع العقاري بمصر:

هدفت الدراسة إلى التعرف على طبيعة الأمن السيبراني وأنظمة محاسبة التكاليف الرقمية في شركات القطاع العقاري بمصر، حيث تعتبر أمن المعلومات وحماية البيانات من التحديات الحيوية التي تواجهها

الشركات في العصر الرقمي، فقد قامت الدراسة بالاعتماد على منهجية تحلل البيانات المجمعة باستخدام أدوات إحصائية الاكتشاف العلاقة بين العوامل المختلفة حيث تساهم الدراسة في تحديد التأثيرات المحتملة لتطبيق أدوات الأمن السيبراني على أنظمة محاسبة التكاليف الرقمية في شركات القطاع العقاري بمصر. وقد توصلت نتائج الدراسة أنه توجد علاقة إحصائية بين الأمن السيبراني على أنظمة التكاليف الرقمية حيث كان هذا الأثر في مجال دقة قياس التكاليف في الشركة التي لا تطبق الأمن السيبراني 0.572 وازداد في الشركة التي تطبق ليصبح 0.741 كما أكد وجود معنوية لتطبيق الأمن السيبراني على أنظمة التكاليف حيث كان هذا الأثر في مجال خفض التكاليف العمومية والإدارية في الشركة التي تطبق الأمن السيبراني 0.648 وازداد في الشركة التي لا تطبق ليصبح 0.737 وأخيراً وجود أثر معنوي لتطبيق الأمن السيبراني على أنظمة التكاليف الرقمية حيث تحسن الربحية في الشركة التي لا تطبق الأمن السيبراني 0.637 وازداد في الشركة التي تطبق ليصبح 0.820.

فقد أوصت الدراسة على الشركات العقارية العمل على تحسين الأمان السيبراني على مستوى الشبكة والأنظمة والتطبيقات ويجب أن تتضمن الجهود التحسينات في تكنولوجيا الحماية، والتدريب للموظفين حول الهجمات السيبرانية المحتملة وكيفية التعامل معها.

2. دراسة (2022, Daoud, & Serag) بعنوان "إطار مقترح لدراسة تأثير الأمن السيبراني على المعلومات المحاسبية لزيادة الثقة في التقارير المالية في سياق الصناعة 4.0: مدخل للحدث والأثر والاستجابة":

يهدف هذا البحث إلى التعرف على إطار مقترح لدراسة تأثير الأمن السيبراني على المعلومات المحاسبية لزيادة الثقة في التقارير المالية في سياق الصناعة وتشمل تقنيات الصناعة البيانات الضخمة وإنترنت الأشياء وتكامل النظام والحوسبة السحابية وRebotics وزيادة الأتمتة والواقع الافتراضي. يساعد الأمن السيبراني في ضمان أن تظل هذه التقنيات والمعلومات الأساسية التي تحتوي عليها للبيع ومحمية. ولقد وجد هذا البحث أن الاتصال البيئي واستخدام جمع البيانات الإلكترونية وتخزينها ونقلها أصبح أكثر انتشاراً، مع اعتماد الصناعة بشكل كبير، مما أدى إلى زيادة عدد الأعمال المستهدفة للسرقة الإلكترونية أو التلف أو التعطل. يعني الأمن السيبراني جميع الخطوات لحماية الأعمال التجارية ضد الاستخدام غير القانوني للبيانات الإلكترونية. وتوصل البحث إلى يمكن للشركات المصنعة أن تظل آمنة ومزدهرة من خلال حماية جميع الأجهزة والبرامج والمعلومات من التهديدات الداخلية والخارجية. هذه الانتهاكات لها آثار على مؤسسات الأعمال أنها قد تؤدي إلى انخفاض الأداء والقيمة السوقية، وزيادة المخاطر التشغيلية

يوصي البحث بضرورة توفير المعلومات والوقت الذي يقضيه الموظف في ضمان الامتثال للوائح الخصوصية والسرية المناسبة.

3. دراسة (عبد السلام عطية عبد السلام يوسف، 2024، بعنوان (تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية الليبية: دراسة وصفية):

يهدف هذا البحث إلى تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية الليبية، كما يهدف البحث إلى تحليل الدراسات السابقة التي تناولت تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية في الوطن العربي وليبيا، وذلك لاستخلاص النتائج والتوصيات المهمة.

تم اعتماد المنهجية الوصفية لهذا البحث، حيث تم اختيار مجموعة من الدراسات السابقة التي بحثت وتعمقت في تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية في الوطن العربي بشكل عام وفي ليبيا بشكل خاص. ستشمل العينة مجموعة متنوعة من الدراسات لباحثين من ذوي الخبرة المهنية في هذه التخصص، وسيتم قراءة وتحليل هذه الدراسات للخروج بمجموعة من النتائج والتوصيات وتوصل البحث إلى أن المؤسسات المالية الليبية تواجه تهديدات سيبرانية متزايدة ومتنوعة، وتشمل هذه التهديدات الاختراقات الهجمات الإلكترونية، سرقة البيانات المالية، التجسس الصناعي، وتعطيل الخدمات المصرفية عبر الإنترنت. هذه التهديدات تسبب تأثيرًا سلبيًا على نظم المعلومات المحاسبية وتمثل خطرًا على السرية والموثوقية والتوافقية. وتوصل البحث إلى أن هناك عدة نقاط ضعف في نظم المعلومات المحاسبية في المؤسسات المالية الليبية، وتشمل هذه النقاط ضعف في رصد وكشف هجمات السيبرانية، نقص في التدريب والوعي الأمني للموظفين، ضعف في إجراءات التحقق والتحكم الداخلي، وعدم وجود استراتيجيات شاملة للأمن السيبراني. كما توصل البحث إلى التهديدات السيبرانية تسبب تأثيرًا اقتصاديًا كبيرًا على المؤسسات المالية الليبية، وتشمل هذه التأثيرات تكاليف استعادة البيانات وإصلاح الأضرار، فقدان الثقة لدى العملاء والمستثمرين، توقف الخدمات المصرفية، وتعرض الشركات للمسائل القانونية والتعويضات المالية وفي الختام، أوصى البحث أن المؤسسات المالية يجب عليها تقييم وتحديث سياسات الأمان والإجراءات المتعلقة بنظم المعلومات المحاسبية لتوفير حماية فعالة ضد التهديدات السيبرانية، كما ينبغي أيضًا تنفيذ نظم رصد وكشف متقدمة للكشف المبكر عن الهجمات السيبرانية والتعامل معها بشكل سريع وفعال. كما ينبغي على

المؤسسات المالية تعزيز التعاون مع الهيئات الحكومية ذات الصلة والمؤسسات الأمنية والخبراء في مجال الأمن السيبراني.

4. دراسة (السرطان وأخرون، المشاقبة، 2020 م، بعنوان "أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية في البنوك التجارية الأردنية":

هدفت الدراسة لبحث أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية في البنوك التجارية الأردنية، تم توزيع الاستبانة على مجتمع الدراسة المتمثل بالبنوك التجارية الأردنية والبنوك التجارية العاملة في الأردن، وتم تحليل المعلومات باستخدام برنامج التحليل الإحصائي SPSS. وخرجت الدراسة بالنتائج التالية: يوجد أثر لخصوصية بيانات العملاء وإدارة المخاطر السيبرانية وتحديد الجهة المالكة ونطاق التطبيق والصلاحيات على جودة المعلومات المحاسبية، وأن خصوصية بيانات العملاء كان لها الأثر الأكبر على جودة المعلومات المحاسبية، وأوصت الدراسة بضرورة زيادة الاهتمام بالحفاظ على خصوصية بيانات العملاء لتعزيز جودة المعلومات المحاسبية، ضرورة اهتمام البنوك بالإفصاح عن الأمن السيبراني في تقاريرها السنوية، وأخيراً تشجيع الباحثين على إجراء دراسات خاصة بالأمن السيبراني.

ما يميز دراستي عن الدراسات السابقة:

بينما تتناول الدراسات السابقة قطاعات متنوعة (العقارات، المؤسسات المالية، البنوك)، تركز دراستي على الشركات الصناعية الليبية، وتحديدًا مصنع أسمنت المرقب. هذا التحديد يمنح دراستي خصوصية وأهمية في فهم التحديات الفريدة التي تواجه هذا القطاع الحيوي في ليبيا.

باختصار، ما يميز دراستي هو:

- التركيز المحدد على الشركات الصناعية الليبية، وتحديدًا مصنع أسمنت المرقب.
- المنهجية الاستطلاعية من وجهة نظر الموظفين في الإدارة المالية.
- العمق والتفصيل في تحليل الوضع الراهن للأمن السيبراني في مصنع أسمنت المرقب.
- حداثة الدراسة.
- المنهجية التطبيقية.

الدراسة الميدانية

تتناول هذه الدراسة وصفاً لمنهج الدراسة الذي استخدمه البحث ، ويرصد حدود الدراسة، ويعين مجتمع الدراسة، وكيفية اختيار العينة، وخصائص أفراد العينة في ضوء سماتهم الديموغرافية، ثم يستعرض بناء الدراسة المستخدمة في جمع البيانات والمعلومات اللازمة للدراسة، والإجراءات التي قام بها البحث للتأكد من مداها الظاهري والبنائي وكذلك للتأكد من ثباتها، كما يتضمن وصفاً للإجراءات التي قام بها البحث في تقنين أدوات الدراسة وتطبيقها، وأخيراً يوضح كيفية تطبيق الدراسة، والأساليب الإحصائية المستخدمة في تحليل بيانات الدراسة.

مجتمع البحث:

يقصد بالمجتمع: المجموعة الكلية من الناس أو الأحداث، أو الأشياء التي يسعى البحث إلى أن يعمم عليها نتائج الدراسة ذات العلاقة بالمشكلة المدروسة (النجار وآخرون، 2020: 86).

يتمثل مجتمع الدراسة (مصنع أسمنت المرقب) في جميع موظفين الإدارة العامة للشؤون المالية، فقد تم حصر ذلك فقط واستخدام عينة مسح شامل والبالغ عددهم 25 مفردة (مدراء إدارات ورؤساء أقسام ووحدات وموظفين) من الموظفين المصنع.

عينة البحث:

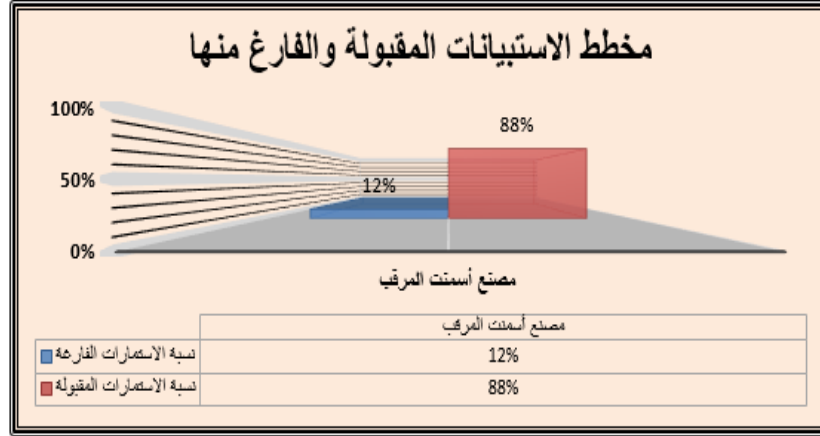
يتم اختيار العينة وفقاً لقواعد خاصة بحيث تمثل المجتمع الذي أخذت منه والذي يجري عليه البحث بمعنى أن تحمل نفس خصائص المجتمع من أجل الحصول على دراسة موضوعية (النعيبي، 2015: 63).

حيث تم توزيع (25) استبانة، استرجع منها (22) استبانة بنسبة 88%، وبعد المراجعة تبين أنها صالحة للمعالجة الإحصائية، ويوضح الجدول التالي توزيع عينة البحث حسب القطاع الموجودة آنفاً:

الجدول (1): تفاصيل الاستبيانات الموزعة والمستردة والفاقد منها لحجم العينة المدروسة

ت	البيان	الاستبيانات الموزعة	الفاغرة	الاستبيانات المقبولة	الفاغرة	الاستبيانات المقبولة	نسبة المقبولة
1	مصنع أسمنت المرقب	25	03	22	12%	88%	
	إجمالي الاستبيانات لعينة البحث	25	03	22	12%	88%	

من الجدول رقم (1) أن نسبة الاستثمارات المسترجعة الكلية 88% من جميع الاستثمارات الموزعة وهي نسبة عالية حسب جدول مورغان الذي يشير إلى أن النسبة المعنوية 12%.



الشكل رقم (1): تفاصيل الاستبيانات المقبولة والفارغ منها لحجم العينة المدروسة

أداة جمع البيانات (الاستبيان):

إن الأداة المستخدمة في جمع المعلومات المراد الحصول عليها من أفراد عينة البحث هي الاستبيان حول موضوع البحث حيث تكونت الاستبيان من 34 فقرة، موزعة على المعلومات الشخصية ومحورين موضحة كما يلي:

أ. المعلومات الشخصية: وتكونت من 4 فقرات هي (المؤهل العلمي – المركز الوظيفي – التخصص – عدد سنوات الخبرة).

ب. محاور الدراسة: وقد تكون من 4 محاور هما:

1. المحور الأول العبارات المتعلقة: تؤثر سياسات التحكم في الوصول على أمن البيانات المالية الحساسة وتكونت من 10 فقرات.

2. المحور الثاني العبارات المتعلقة: يتم تحديد وقياس فعالية استراتيجيات استجابة الحوادث عند حدوث خرق بيانات وتكونت من 10 فقرات.

3. المحور الثالث العبارات المتعلقة: يتم استخدام تحليل البيانات للكشف عن نقاط الضعف في نظم المعلومات المحاسبية وتكونت من 10 فقرات.

ثبات وصدق الأداة (الاستبيان):

يعتبر الصدق والثبات أداة البحث من أهم الموضوعات التي تهتم الباحثان من حيث تأثيرها البالغ في أهمية نتائج البحث وقدرته على تعميم النتائج، وترتبط الصدق والثبات بالأدوات المستخدمة في البحث ومدى قدرتها على قياس المراد قياسه ومدى دقة القراءات المأخوذة من الأدوات (محمود، 2019: 141).

1. اختبار الثبات:

أما ثبات أداة البحث فيعني التأكد من أن الإجابة ستكون واحدة تقريباً لو تكرر تطبيقها على الأشخاص ذاتهم في أوقات أخرى (العساف، 2014: 430) وقد قام الباحثان بإجراء خطوات الثبات على العينة بطريقتين هما طريقة التجزئة النصفية ومعامل ألفا كرونباخ.

1.1. اختبار الثبات بطريقة التجزئة النصفية (معامل سيرومان براون):

تم إيجاد معامل ارتباط بيرسون بين معدل الأسئلة الفردية الرتبة ومعدل الأسئلة الزوجية الرتبة لكل محور وقد تم تصحيح معاملات الارتباط باستخدام معامل ارتباط سيرومان براون للتصحيح حسب المعادلة وقد بين الجدول رقم (2.2.3) أن هناك معامل ثبات كبير نسبياً لفقرات الاستبانة، حيث يشير (Saunders, Lewis, & Thornhill, 2009:135) إلى أن الثبات المقبول ينبغي ألا يقل عن 0.60%، مما يطمئن الباحثان على استخدام الاستبانة بكل طمأنينة.

الجدول رقم (2): تفاصيل يبين معامل الثبات (طريقة التجزئة النصفية) للمحاور (المصدر: اعتماداً على مخرجات SPSS)

م	المحاور	عدد الفقرات	معامل الارتباط قبل التصحيح	معامل سيرومان براون	النتيجة
1	المحور الأول	07	0.647	804.0	عالي جداً
2	المحور الثاني	07	0.632	0.795	عالي جداً
3	المحور الثالث	07	0.745	0.863	عالي جداً
	الاستبيان ككل	21	6810.	0.825	عالي

من خلال الجدول رقم (2) نلاحظ أنه تقسيم فقرات (تحليل الأمن السيبراني في نظم المعلومات المحاسبية وتأثيره على حماية البيانات المالية الحساسة للشركات الصناعية الليبية) - المحور الأول (تؤثر سياسات التحكم في الوصول على أمن البيانات المالية الحساسة) البالغة (07) فقرات إلى قسمين:

البنود الفردية والبنود الزوجية (4 فردية – 3 زوجية)، حيث يتحصل المبحوث على درجتين إحداهما على النصف الفردي والأخرى على النصف الزوجي، ثم حساب معامل الارتباط بيرسون بينهما، حيث بلغ $RP=0.647$ وبعد تصحيح طوله في معادلة سبيرمان براون بلغ (0.804) وهي قيمة عالية جداً وأكبر من 0.60 وهذا يدل على توفر درجة عالية من الثبات الداخلي في الإجابات مما يمكننا من الاعتماد على إجابات مفردات العينة في تحقيق أهداف البحث ونتائجها.

كذلك نلاحظ أنه تقسيم فقرات المحور الثاني (يتم تحديد وقياس فعالية استراتيجيات استجابة الحوادث عند حدوث خرق بيانات) البالغة (07) فقرات إلى قسمين: البنود الفردية والبنود الزوجية (4 فردية – 3 زوجية)، حيث يتحصل المبحوث على درجتين إحداهما على النصف الفردي والأخرى على النصف الزوجي، ثم تم حساب معامل الارتباط بيرسون بينهما، حيث بلغ $RP=0.632$ وبعد تصحيح طوله في معادلة سبيرمان براون بلغ (0.795) وهي قيمة عالية أكبر من 0.60 وهذا يدل على توفر درجة عالية من الثبات الداخلي في الإجابات مما يمكننا من الاعتماد على إجابات مفردات العينة في تحقيق أهداف البحث ونتائجها.

كذلك نلاحظ أنه تقسيم فقرات المحور الثالث (يتم استخدام تحليل البيانات للكشف عن نقاط الضعف في نظم المعلومات المحاسبية) البالغة (07) فقرات إلى قسمين: البنود الفردية والبنود الزوجية (4 فردية – 3 زوجية)، حيث يتحصل المبحوث على درجتين إحداهما على النصف الفردي والأخرى على النصف الزوجي، ثم تم حساب معامل الارتباط بيرسون بينهما، حيث بلغ $RP=0.745$ وبعد تصحيح طوله في معادلة سبيرمان براون بلغ (0.863) وهي قيمة عالية أكبر من 0.60 وهذا يدل على توفر درجة عالية من الثبات الداخلي في الإجابات مما يمكننا من الاعتماد على إجابات مفردات العينة في تحقيق أهداف البحث ونتائجها.

كذلك نلاحظ أنه تقسيم فقرات الاستبيان ككل البالغة (21) فقرة إلى قسمين: البنود الفردية والبنود الزوجية (12 فردية – 9 زوجية)، حيث يتحصل المبحوث على درجتين إحداهما على النصف الفردي والأخرى على النصف الزوجي، ثم تم حساب معامل الارتباط بيرسون بينهما، حيث بلغ $RP=0.681$ وبعد تصحيح طوله في معادلة سبيرمان براون بلغ (0.825) وهي قيمة عالية أكبر من 0.60 وهذا يدل على توفر درجة عالية من الثبات الداخلي في الإجابات مما يمكننا من الاعتماد على إجابات مفردات العينة في تحقيق أهداف البحث ونتائجها.

1.2. اختبار الثبات بطريقة ألفا كرونباخ Alpha Cronbach's:

يشير الثبات Reliability إلى مدى الموثوقية في المقياس لتحقيق نفس النتائج عند إعادة استخدامه مرة أخرى، بعد فترة من الزمن، لنفس الاستقصاء منهم وفي نفس ظروف الاختبار الأول؛ ويمكن تقييم ذلك بعدة طرق ومن أهمها حساب معامل ألفا كرونباخ، حيث تتراوح قيم ألفا كرونباخ من صفر (عناصر غير ثابتة) إلى واحد صحيح (ثبات تام)، ويكون معامل الثبات مقبولاً إذا كان أكبر من (0.60) وضعيفاً إذا كان أقل من ذلك وعن طريق استخدام حساب معاملات الارتباط بين كل فقرة من الفقرات في الاستبانة عن طريق استخدام معامل (ألفا كرونباخ). فكلما كان هذا البعد عالياً دل ذلك على ثبات وموثوقية نتائجه، وبالتالي كان المقياس مقبولاً ويمكن الاعتماد عليه.

الجدول رقم (3): نتائج اختبار الثبات (معامل ألفا كرونباخ) لمحاور الاستبيان (المصدر: اعتماداً على مخرجات spss)

م	المحاور	عدد الفقرات	معامل الثبات (قيمة معامل ألفا كرونباخ)	النتيجة
1	المحور الأول	07	752.0	عالي
2	المحور الثاني	07	0.817	عالي جداً
3	المحور الثالث	07	0.796	عالي
	الاستبيان ككل	21	6910.	عالي

يتضح من الجدول (3) أن قيمة معامل الثبات لمعامل ألفا كرونباخ Cronbach -Alpha للمحاور قد تراوحت بين (0.691- 0.817) وهي معاملات عالية وتتمتع بدرجة جيدة من الثبات، كذلك قيمة معامل الثبات لمعامل ألفا كرونباخ Cronbach -Alpha للاتساق الداخلي لأداة البحث بلغ (0.691) وهو معامل عالي جداً، وبذلك يعتبر هذا المقياس صادقاً لما وضع للقياس، وكما يتمتع بدرجة عالية وممتازة من الثبات مقارنة بالمستوى المقبول (0.60) وهو الحد الأدنى المقبول لثبات أي مقياس في العلوم الإدارية، وبالتالي يمكن الاعتماد عليه في التطبيق مما يجعل استمارة الاستبيان مقبولة كأداة لجمع البيانات اللازمة للبحث.

2. اختبار الصدق:

اختبار صدق الاستبانة يعني التأكد من أنها سوف تقيس ما أعدت لقياسه (العساف، 2013: 429)، كما يقصد بالصدق "شمول الاستبانة لكل العناصر التي يجب أن تدخل في التحليل من ناحية، ووضوح فقراتها ومفرداتها من ناحية ثانية، بحيث تكون مفهومة لكل من يستخدمها" (عبيدات وآخرون، 2015: 179)، وقد قام الباحثان بالتأكد من صدق أداة البحث كما يلي:

- **صدق فقرات الاستبانة:** تم التأكد من صدق فقرات الاستبانة بطريقتين وهما:

1. **الصدق الظاهري للأداة البحث (صدق المحكمين):** للتحقق من صدق الأداة اعتماداً على الباحثان صدق المحتوى إذ قام بعرض الأداة على محكمين من ذوي الاختصاص في مجال المحاسبة وذلك بغرض معرفة ما تقيسه الفقرات من الأداء المطلوب ومدى صلة فقرات المقياس بالمتغير المراد قياسه، وللحكم على الفقرات وصياغتها ودرجة وضوحها، ومناسبتها للمجالات وقد أخذ الباحثان بملاحظات المحكمين فحذف بعض العبارات وأضاف عبارات أخرى حسب توجيهاتهم.

2. **صدق الاتساق الداخلي والبنائي لمحاور البحث:** يشير الصدق Validity في هذا البحث تم إجراء اختبار الصدق الداخلي وهو الذي يقيس الاتساق الداخلي لعبارات البعد الواحد مع بعضها البعض، ويُعرف ذلك من خلال الجذر التربيعي لقيمة معامل ألفا كرونباخ. وكذلك تم إجراء اختبار الصدق البنائي والذي يهتم بصلاحية بناء المقياس بمعرفة درجة ترابط محاوره بالدرجة الكلية للمقياس، ويُعرف ذلك من خلال معامل ارتباط بيرسون، والذي ينبغي ألا يقل عن (0.35) وفقاً ل (Netemeyer, Bearden, & Sharma, 2003) وفيما يلي نتائج ذلك:

جدول رقم (4): نتائج اختبارات الصدق لمحاور الاستبيان (المصدر: اعتماداً على مخرجات SPSS)

م	المحاور	معامل الصدق البنائي (الارتباط مع الدرجة الكلية للاستبيان)	معامل الصدق الداخلي (الاتساق الداخلي) الجذر التربيعي لمعامل ألفا كرونباخ	مستوى الدلالة	النتيجة
1	المحور الأول	0.745**	0.863	0.000	عالي جداً
2	المحور الثاني	0.685**	0.828	0.000	عالي جداً
3	المحور الثالث	0.823**	0.907	0.000	عالي جداً
	الاستبيان ككل	0.739**	0.859		عالي جداً

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

من الجدول (4) يتضح أن محاور أداة البحث (الاستبيان)، حققت درجة الصدق المطلوب، كما هو واضح من معاملات الصدق البنائي والصدق الداخلي، والتي كانت دالة إحصائياً وجميعها عند درجة دلالة 0.01، سواءً بالنسبة للمحاور أو المتغيرات، وبالتالي يمكن الاعتماد على الأداة في قياس متغيرات البحث، وتحقيق أهدافه.

• اختبار التوزيع الطبيعي **Normality Test**: تم استخدام اختبار كولمجروف - سمرنوف - One sample K-s Test لمعرفة هل البيانات تتبع التوزيع الطبيعي أم لا، وهو اختبار ضروري في حالة اختبار الفرضيات، لأن أغلب الاختبارات المعملية يشترط فيها أن تكون البيانات موزعة توزيعاً طبيعياً (Pallant، 2007:40).

أن الجدول رقم (5) يوضح نتائج اختبار كولمجروف - سمرنوف حيث يبين أن القيمة الإحصائية وقيمة مستوى الدلالة لكل المتغيرات أكبر من 0.05 ($\text{sig} > 0.05$) وهذا يدل على أن البيانات تتبع التوزيع الطبيعي ويجب استخدام الاختبارات المعملية.

جدول رقم (5): تفاصيل اختبار التوزيع الطبيعي (One-Sample K-S Test) (المصدر: اعتماداً على مخرجات spss)

م	المحاور	القيمة الإحصائية	درجة الحرية	الدلالة المعنوية
1	المحور الأول	0.124	22	0.054
2	المحور الثاني	0.129	22	0.062
3	المحور الثالث	0.131	22	0.068
	الاستبيان ككل	0.127	22	058.0

* This is a lower bound of the true significance.

a. Lilliefors Significance Correction

يتضح من الجدول (5) أن قيمة مستوى الدلالة المعنوية الاستبيان ككل كانت 0.058 عند مستوى دلالة إحصائية أكبر من مستوى ($\alpha \leq 0.05$) وهذا يعني أن فقرات ومحاور البحث تخضع للتوزيع الطبيعي ويجب استخدام الاختبارات المعملية عليها.

• المعالجات الإحصائية:

قام الباحثان باستخدام مجموعة من الأساليب الإحصائية في عملية التحليل الإحصائي من خلال برنامج (SPSS) وهي: التكرارات والنسب المئوية -الأوساط الحسابية والانحرافات المعيارية -اختبار ألفا كرونباخ لمعرفة ثبات فقرات الاستبانة -اختبار معامل الارتباط (بيرسون) لمعرفة العلاقة بين المتغيرات ودرجتها وقوتها -اختبار التوزيع الطبيعي لمعرفة هل البيانات تتبع التوزيع الطبيعي أم لا.

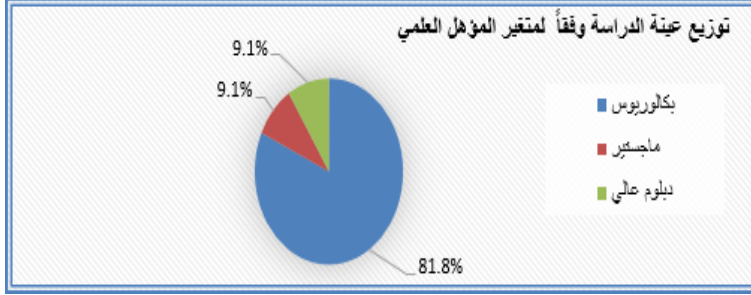
• خصائص عينة البحث:

1. خصائص عينة الدراسة وفقاً للمؤهل العلمي:

الجدول رقم (6): خصائص عينة الدراسة وفقاً للمؤهل العلمي (من إعداد الباحثان اعتماداً على مخرجات برنامج (SPSS))

الترتيب حسب التوافر	النسبة	التكرار	المؤهل العلمي
1	81.8%	18	بكالوريوس
2	9.1%	02	ماجستير
3	9.1%	02	دبلوم عالي
-	%100	22	الإجمالي

من خلال البيانات الواردة في الجدول رقم (6) يتبين أن الموظفين من حملة البكالوريوس هم أكثر المستجوبين تكراراً وتوافراً بالعينة، وبنسبة وصلت إلى (81.8%) من حجم العينة، في حين كانت نسبة حجم العينة من حملة الماجستير، بنسبة وصلت إلى (9.1%)، في حين كانت نسبة حجم العينة من حملة الدبلوم العالي، بنسبة وصلت إلى (9.1%) وهذه النسب واقعية حيث أن أكثر أفراد المجتمع متعلمين وحملة شهادات من ناحية، ومن ناحية أخرى تتوافق هذه النسب مع توزيع حجم العينة، وغالبية هذه الفئة هم حملة شهادة البكالوريوس، وبالتالي فالعينة هنا ممثلة للمؤهلات التعليمية لمجتمع الدراسة. والشكل التالي رقم (2) يوضح ذلك:



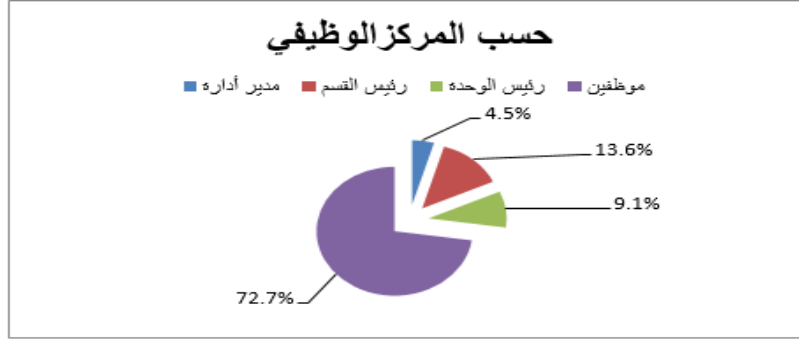
شكل رقم (2): توزيع عينة الدراسة وفقاً للمؤهل العلمي

2. خصائص عينة الدراسة وفقاً للمركز الوظيفي:

الجدول رقم (7): خصائص عينة المركز الوظيفي (من إعداد الباحثان اعتماداً على مخرجات برنامج (SPSS))

المركز الوظيفي	التكرار	النسبة	الترتيب حسب التوافر
مدير إدارة	01	4.5%	4
رئيس القسم	03	13.6%	2
رئيس الوحدة	02	9.1%	3
موظفين	16	72.7%	1
الإجمالي	22	100%	-

من خلال البيانات الواردة في الجدول رقم (7) يتبين أن نسبة الموظفين وصلت نسبتهم إلى (72.7%) من حجم العينة هم أكبر نسبة، في حين كانت نسبة رئيس القسم نسبتهم وصلت إلى (13.6%)، في حين كانت نسبة رئيس الوحدة نسبتهم وصلت إلى (9.1%)، في حين كانت نسبة مدير الإدارة نسبتهم وصلت إلى (4.5%)، وهذه النسب واقعية حيث أن أكثر أفراد المجتمع متعلمين وحملة شهادات من ناحية، ومن ناحية أخرى تتوافق هذه النسب مع توزيع حجم العينة، وغالبية هذه الفئة هم حملة شهادة البكالوريوس، وبالتالي فالعينة هنا ممثلة للمؤهلات التعليمية لمجتمع الدراسة. والشكل التالي رقم (3) يوضح ذلك:



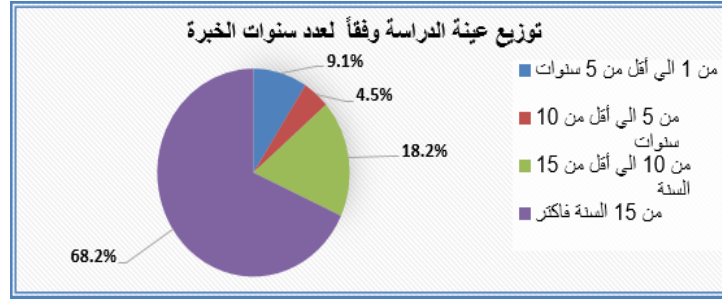
شكل رقم (3): توزيع عينة الدراسة وفقاً للمركز الوظيفي

3. خصائص عينة الدراسة وفقاً لسنوات الخبرة:

الجدول رقم (8): خصائص عينة الدراسة وفقاً لسنوات الخبرة (من إعداد الباحثان اعتماداً على مخرجات برنامج (SPSS))

سنوات الخبرة	التكرار	النسبة	الترتيب حسب التوافر
من 1 إلى أقل من 5 سنوات	02	9.1%	3
من 5 إلى أقل من 10 سنوات	01	4.5%	4
من 10 إلى أقل من 15 سنة	04	18.2%	2
من 15 سنة فأكثر	15	68.2%	1
الإجمالي	22	100%	-

من خلال البيانات الواردة في الجدول رقم (8) يتبين أن الموظفين لخبرتهم من 15 سنة هم أكثر المستجوبين تكراراً وتوافراً بالعينة، وبنسبة وصلت إلى (68.2%) من حجم العينة، في حين كانت نسبة الذين خبرتهم من 10 إلى 15 سنة، بنسب وصلت إلى (18.2%)، في حين كانت نسبة الذين خبرتهم من 1 إلى 5 سنوات، بنسب وصلت إلى (9.1%)، في حين كانت نسبة الذين خبرتهم من 5 إلى أقل من 10 سنوات، بنسب وصلت إلى (4.5%) وهذه النسب واقعية حيث أن أكثر أفراد المجتمع خبرتهم عالية والشكل التالي رقم (4) يوضح ذلك:



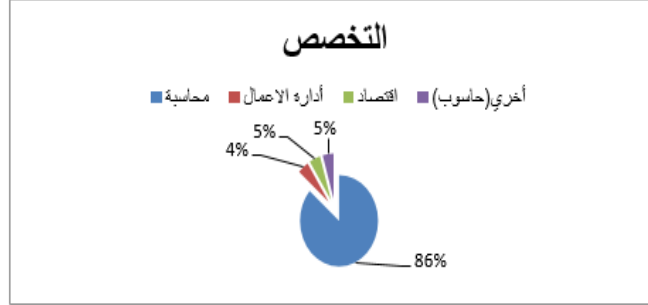
شكل رقم (4): توزيع عينة الدراسة وفقاً لسنوات الخبرة

4. توزيع مفردات مجتمع الدراسة حسب التخصص:

الجدول رقم (9): يبين التوزيع التكراري والنسبي المئوي لمفردات مجتمع الدراسة حسب التخصص (من إعداد الباحثان اعتماداً على مخرجات برنامج (SPSS))

الترتيب حسب التوافر	النسبة	التكرار	التخصص
1	86.4%	19	محاسبة
2	4.5%	01	إدارة الأعمال
3	4.5%	01	اقتصاد
4	4.5%	01	أخرى (حاسوب)
-	100%	22	الإجمالي

من خلال الجدول (9) نلاحظ أن معظم مفردات مجتمع الدراسة كانت أعلى نسبة هي فئة تخصصهم محاسبة ويمثل نسبة 86.4% من جميع مفردات مجتمع الدراسة، ثم يليه الذين تخصصهم إدارة الأعمال بنسبة 4.5% من عينة الدراسة، ويليه من تخصصهم اقتصاد وكانت النسبة 4.5%، ويليه من تخصصهم أخرى (حاسوب) وكانت النسبة 4.5%، نلاحظ أن تخصصهم محاسبة أعلى نسبة في مجال العمل وهذا يضمن البحث في صدق إعطاء الإجابات والشكل التالي رقم (5) يوضح ذلك:



شكل رقم (5): توزيع عينة الدراسة وفقاً للتخصص

• التحليل الوصفي لإجابات عينة البحث:

تم تحليل إجابات عينة البحث على فقرات أداة البحث (الاستبيان) بالاعتماد على المتوسطات الحسابية والانحرافات المعيارية وذلك لتحديد درجة الموافقة، وقد اعتمدت أداة البحث مقياس ليكارث الخماسي، حيث كانت الدرجة 5 تعني موافق بشدة، والدرجة 1 تعني غير موافق بشدة، وقد تم احتساب المدى المتوسط للحكم على درجة الموافقة كما هو موضح بالجدول (10) التالي: (Pimentel, 2010 : 110)

الجدول رقم (10): مقياس درجة الموافقة وفق مقياس ليكارث الخماسي للمتوسطات الحسابية (المصدر: اعتماداً على مخرجات برنامج (SPSS))

القياس	الدرجة	المتوسط المرجح	درجة الموافقة
لا أوافق تماماً	1	من 1:00 إلى 1.80	منخفضة جداً
لا أوافق	2	أكثر من 1.80 إلى 2.60	منخفضة
محايد	3	أكثر من 2.60 إلى 3.40	متوسطة
أوافق	4	أكثر من 3.40 إلى 4.20	مرتفعة
أوافق تماماً	5	أكثر من 4.20 إلى 5.00	مرتفعة جداً

حيث تم ذلك وفقاً للعمليات الحسابية الآتية:

1. تم احتساب المدى في مقياس ليكارث الخماسي المدى $4 = 1 - 5$

2. ثم قسمة المدى (4) على أكبر قيمة وهي (5) حسب الآتي: $0.80 = 5 \div 4$

3. تم إضافة هذه القيمة (0.80) إلى أقل قيمة وهي (1)، وهكذا حسب ما هو موضح في الجدول أعلاه رقم (10).

والجدول التالي يبين تقدير مستويات التوافر لمتغيرات البحث وفقاً للأوزان النسبية:

جدول رقم (11): تقدير مستويات التوافر لمتغيرات البحث وفقاً للأوزان النسبية (المصدر: اعتماد على مخرجات SPSS)

معدل الوزن النسبي	100-90	89.9-80	79.9-70	69.9-50	أقل من 50
التقدير	ممتاز جداً	جيد جداً	جيد	مقبول	ضعيف

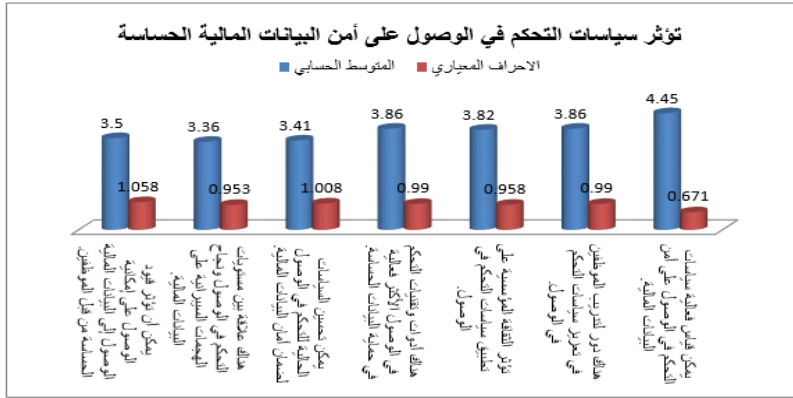
وفيما يلي التحليل الوصفي لإجابات عينة البحث لمحاوّر متغيرات البحث كلّ على حدة:

تحليل الأمن السيبراني في نظم المعلومات المحاسبية وتأثيره على حماية البيانات المالية الحساسة للشركات الصناعية الليبية. دراسة ميدانية على مصنع أسمنت المرقب.

المحور الأول: تحليل إجابات عينة البحث حول تأثير سياسات التحكم في الوصول على أمن البيانات المالية الحساسة.

الجدول (12): يوضح تحليل البيانات حول وجود تأثير سياسات التحكم في الوصول على أمن البيانات المالية الحساسة (المصدر: اعتماد على مخرجات SPSS)

تؤثر سياسات التحكم في الوصول على أمن البيانات المالية الحساسة					
ت	الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	درجة الموافقة
1	يمكن أن تؤثر قيود الوصول على إمكانية الوصول إلى البيانات المالية الحساسة من قبل الموظفين.	3.50	1.058	70.0%	مرتفع
2	هناك علاقة بين مستويات التحكم في الوصول ونجاح الهجمات السيبرانية على البيانات المالية.	3.36	0.953	67.3%	متوسط
3	يمكن تحسين السياسات الحالية للتحكم في الوصول لضمان أمن البيانات المالية.	3.41	1.008	68.2%	متوسط
4	هناك أدوات وتقنيات التحكم في الوصول الأكثر فعالية في حماية البيانات الحساسة.	3.86	0.990	77.3%	مرتفع
5	تؤثر الثقافة المؤسسية على تطبيق سياسات التحكم في الوصول.	3.82	0.958	76.4%	مرتفع
6	هناك دور لتدريب الموظفين في تعزيز سياسات التحكم في الوصول.	3.86	0.990	77.3%	مرتفع
7	يمكن قياس فعالية سياسات التحكم في الوصول على أمن البيانات المالية.	4.45	0.671	89.1%	مرتفع
المتوسط والانحراف والوزن النسبي العام		3.87	0.594	77.4%	مرتفع



شكل رقم (6): توزيع عينة البحث وفقاً لتأثير سياسات التحكم في الوصول على أمن البيانات المالية الحساسة

يتبين من الجدول رقم (12) والشكل رقم (6) المتوسطات الحسابية والانحرافات المعيارية والأوزان النسبية لإجابات العينة حول (تأثير سياسات التحكم في الوصول على أمن البيانات المالية الحساسة)، وقد تراوحت بين المتوسط والارتفاع.

فقد جاء في الترتيب الأول الفقرة رقم (7) بمتوسط حسابي مقداره (4.45) وهو متوسط مرتفع، وبانحراف معياري (0.671) وقد بلغ الوزن النسبي (89.1%) مما يدل أن مستوى الفقرة تقديره جيد ودرجة الموافقة لدى العينة مرتفعة يشير إلى تشتت الآراء وتباينها حول الفقرة، وبالتالي توافر مقتضاها جيد يمكن قياس فعالية سياسات التحكم في الوصول على أمن البيانات المالية "بدرجة عالية".

في حين جاءت الفقرة رقم (2) في الترتيب الأخير من حيث درجة الموافقة عليها، فقد بلغ متوسطها الحسابي (3.36)، وبانحراف معياري (0.953) وقد بلغ الوزن النسبي (67.3%) مما يدل أن مستوى الفقرة (هناك علاقة بين مستويات التحكم في الوصول ونجاح الهجمات السيبرانية على البيانات المالية) تقديره متوسط ودرجة الموافقة لدى العينة متوسطة يشير إلى تشتت الآراء وتباينها حول الفقرة، وكل ذلك يدل على أنّ درجة الموافقة على الفقرة متوسطة، وبالتالي توافر مقتضاها بدرجة متوسطة من وجهة نظر عينة البحث.

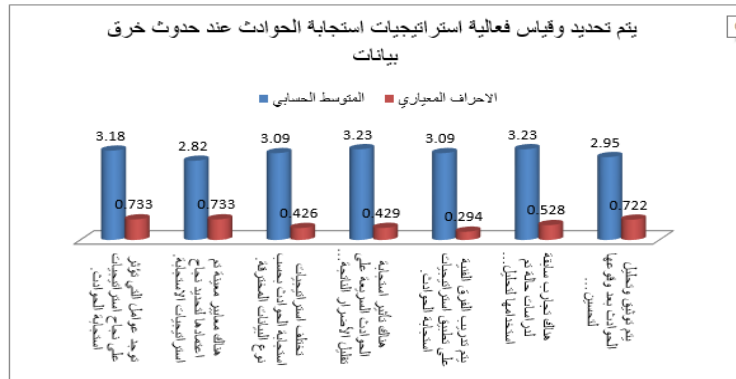
وبشكل عام نجد أن لتأثير سياسات التحكم في الوصول على أمن البيانات المالية الحساسة لدى عينة الدراسة، متوفرة بدرجة مرتفعة، من وجهة نظر أولئك الموظفين، حيث حصل هذا المحور على متوسط حسابي عام (3.75) وهو متوسط مرتفع، وانحراف معياري (0.724)، ووزن النسبي (75%) بمستوى توافر

تقديره جيد جداً مما يدل على أنّ مستوى المحور لدى عينة الدراسة في مجتمع الدراسة جيدة من وجهة نظر موظفين عينة الدراسة.

المحور الثاني: تحليل إجابات عينة البحث حول يتم تحديد وقياس فعالية استراتيجيات استجابة الحوادث عند حدوث خرق بيانات:

الجدول (13): يوضح تحليل البيانات حول يتم تحديد وقياس فعالية استجابة الحوادث عند حدوث خرق بيانات (المصدر: اعتماد على مخرجات SPSS)

يتم تحديد وقياس فعالية استراتيجيات استجابة الحوادث عند حدوث خرق بيانات						
الترتيب	درجة الموافقة	الوزن النسبي	الانحراف المعياري	المتوسط الحسابي	الفقرة	ت
3	متوسط	63.6%	0.733	3.18	توجد عوامل التي تؤثر على نجاح استراتيجيات استجابة الحوادث.	1
7	ضعيف	56.4%	0.733	2.82	هناك معايير معينة تم اعتمادها لتحديد نجاح استراتيجيات الاستجابة.	2
4	متوسط	61.8%	0.426	3.09	تختلف استراتيجيات استجابة الحوادث بحسب نوع البيانات المخترقة.	3
2	متوسط	64.5%	0.429	3.23	هناك تأثير استجابة الحوادث السريعة على تقليل الأضرار الناتجة عن خرق البيانات.	4
5	متوسط	61.8%	0.294	3.09	يتم تدريب الفرق الفنية على تطبيق استراتيجيات استجابة الحوادث.	5
1	متوسط	64.5%	0.528	3.23	هناك تجارب سابقة لدراسات حالة تم استخدامها لتحليل فعالية هذه الاستراتيجيات.	6
6	ضعيف	59.1%	0.722	2.95	يتم توثيق وتحليل الحوادث بعد وقوعها لتحسين الاستراتيجيات في المستقبل.	7
متوسط		61.6%	0.375	3.08	المتوسط والانحراف والوزن النسبي العام	



شكل رقم (7): توزيع عينة البحث وفقاً يتم تحديد وقياس فعالية استراتيجيات استجابة الحوادث عند حدوث خرق بيانات

يتبين من الجدول رقم (13) والشكل (7) المتوسطات الحسابية والانحرافات المعيارية والأوزان النسبية لإجابات العينة حول وفقاً يتم تحديد وقياس فعالية استراتيجيات استجابة الحوادث عند حدوث خرق بيانات، وقد تراوحت بين المتوسط والارتفاع.

فقد جاء في الترتيب الأول الفقرة رقم (6) بمتوسط حسابي مقداره (3.23) وهو متوسط مرتفع، وبانحراف معياري (0.528) وقد بلغ الوزن النسبي (64.5%) مما يدل أن مستوى الفقرة تقديره جيد ودرجة الموافقة لدى العينة مرتفعة يشير إلى تشتت الآراء وتباينها حول الفقرة، وبالتالي توافر مقتضاها جيد "هناك تجارب سابقة لدراسات حالة تم استخدامها لتحليل فعالية هذه الاستراتيجيات" بدرجة جيدة.

في حين جاءت الفقرة رقم (02) في الترتيب الأخير من حيث درجة الموافقة عليها، فقد بلغ متوسطها الحسابي (2.82)، وبانحراف معياري (0.733) وقد بلغ الوزن النسبي (56.4%) مما يدل أن مستوى الفقرة هناك معايير معينة تم اعتمادها لتحديد نجاح استراتيجيات الاستجابة، تقديره ضعيف جدا ودرجة الموافقة لدى العينة ضعيفة يشير إلى تشتت الآراء وتباينها حول الفقرة، وكل ذلك يدل على أن درجة الموافقة على الفقرة ضعيفة، وبالتالي توافر مقتضاها بدرجة ضعيفة من وجهة نظر عينة البحث.

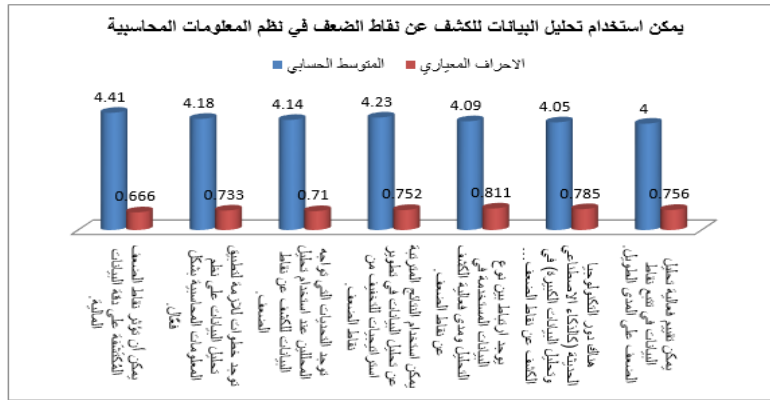
وبشكل عام نجد أن تحديد وقياس فعالية استراتيجيات استجابة الحوادث عند حدوث خرق بيانات من وجهة نظر الموظفين، متوفرة بدرجة جيدة، حيث حصل هذا المحور على متوسط حسابي عام (3.08) وهو متوسط محايد، وانحراف معياري (0.375)، ووزن النسبي (61.6%) بمستوى وجود تقديره محايد مما يدل

على أنّ المحور كانت الإجابات أغلبها بالتحديد وهذا يدل على عدم تحديد وقياس فعالية استراتيجيات استجابة الحوادث عند حدوث خرق بيانات لدى المصنع من وجهة نظر عينة الدراسة.

المحور الثالث: تحليل إجابات عينة البحث يمكن استخدام تحليل البيانات للكشف عن نقاط الضعف في نظم المعلومات المحاسبية:

الجدول (14): يوضح تحليل البيانات حول يمكن استخدام تحليل البيانات للكشف عن نقاط الضعف في نظم المعلومات المحاسبية (المصدر: اعتماد على مخرجات SPSS)

يمكن استخدام تحليل البيانات للكشف عن نقاط الضعف في نظم المعلومات المحاسبية						
الترتيب	درجة الموافقة	الوزن النسبي	الانحراف المعياري	المتوسط الحسابي	الفقرة	ت
1	مرتفع	88.2%	0.666	4.41	يمكن أن تؤثر نقاط الضعف المُكتشفة على دقة البيانات المالية.	1
3	مرتفع	83.6%	0.733	4.18	توجد خطوات اللازمة لتطبيق تحليل البيانات على نظم المعلومات المحاسبية بشكل فعال.	2
4	مرتفع	82.7%	0.710	4.14	توجد التحديات التي تواجه المحللين عند استخدام تحليل البيانات للكشف عن نقاط الضعف.	3
2	مرتفع	84.5%	0.752	4.23	يمكن استخدام النتائج المترتبة عن تحليل البيانات في تطوير استراتيجيات للتخفيف من نقاط الضعف.	4
5	مرتفع	81.8%	0.811	4.09	يوجد ارتباط بين نوع البيانات المستخدمة في التحليل ومدى فعالية الكشف عن نقاط الضعف.	5
6	مرتفع	80.9%	0.785	4.05	هناك دور التكنولوجيا الحديثة (كالذكاء الاصطناعي وتحليل البيانات الكبيرة) في الكشف عن نقاط الضعف في نظم المعلومات المحاسبية.	6
7	مرتفع	80.0%	0.756	4.00	يمكن تقييم فعالية تحليل البيانات في تتبع نقاط الضعف على المدى الطويل.	7
	عالي	83%	0.613	4.15	المتوسط والانحراف والوزن النسبي العام	



شكل رقم (8): توزيع عينة البحث يمكن استخدام تحليل البيانات للكشف عن نقاط الضعف في نظم المعلومات المحاسبية

يتبين من الجدول رقم (14) والشكل (8) المتوسطات الحسابية والانحرافات المعيارية والأوزان النسبية لإجابات العينة حول يمكن استخدام تحليل البيانات للكشف عن نقاط الضعف في نظم المعلومات المحاسبية، وقد تراوحت بين المتوسط والارتفاع.

فقد جاء في الترتيب الأول الفقرة رقم (1) بمتوسط حسابي مقداره (4.41) وهو متوسط مرتفع، وبانحراف معياري (0.660) وقد بلغ الوزن النسبي (88.2%) مما يدل أن مستوى الفقرة تقديره ممتاز ودرجة الموافقة لدى العينة مرتفعة يشير إلى تشتت الآراء وتباينها حول الفقرة، وبالتالي توافر مقتضاها جيد يمكن أن تؤثر نقاط الضعف المُكشَّفة على دقة البيانات المالية "بدرجة عالية".

في حين جاءت الفقرة رقم (7) في الترتيب الأخير من حيث درجة الموافقة عليها، فقد بلغ متوسطها الحسابي (4.0)، وبانحراف معياري (0.756) وقد بلغ الوزن النسبي (80%) مما يدل أن مستوى الفقرة (يمكن تقييم فعالية تحليل البيانات في تتبع نقاط الضعف على المدى الطويل) تقديره جيد جداً ودرجة الموافقة لدى العينة جيدة يشير إلى تشتت الآراء وتباينها حول الفقرة، وكل ذلك يدل على أنّ درجة الموافقة على الفقرة جيدة، وبالتالي توافر مقتضاها بدرجة متوسطة من وجهة نظر عينة البحث.

وبشكل عام نجد محور، يمكن استخدام تحليل البيانات للكشف عن نقاط الضعف في نظم المعلومات المحاسبية، متوفرة بدرجة جيدة، حيث حصل هذا المحور على متوسط حسابي عام (4.15) وهو متوسط مرتفع، وانحراف معياري (0.479)، ووزن النسبي (83%) بمستوى تقديره جيد مما يدل على أنّ المحور

مرتفع من وجهة نظر عينة الدراسة وحسب التكرارات نجد أن أغلب إجابات عينة الدراسة بأنه يمكن استخدام تحليل البيانات للكشف عن نقاط الضعف في نظم المعلومات المحاسبية.

اختبار فرضيات الدراسة

وفيما يلي اختبار الفرضية الرئيسية والفرضيات الفرعية للفرضية الرئيسية:

ومن أجل قبول هذه الفرضية أو نفيها يتطلب الأمر معرفة يؤثر تحليل الأمن السيبراني على حماية البيانات المالية الحساسة في نظم المعلومات المحاسبية في الشركة الأهلية للأسمت المساهمة (مصنع أسمنت المرقب) ولمعرفة ذلك تم استخدام نموذج اختبار (T-test)، وكانت النتائج كما هي في الجدول رقم (15):

جدول رقم (15): نتائج اختبار (T-test) لبيان يؤثر تحليل الأمن السيبراني على حماية البيانات المالية الحساسة في نظم المعلومات المحاسبية محل الدراسة

المجال	المتوسط الحسابي	الفرق بين متوسط الفقرة والمتوسط المعياري	الانحراف المعياري	القيمة الإحصائية / T-Test	قيمة الدلالة الإحصائية	معنوية العلاقة
الفرضية الأولى	3.75	0.75	0.724	4.875	0.000	معنوي
الفرضية الثانية	3.08	0.08	0.375	1.054	0.304	غير معنوي
الفرضية الثالثة	4.15	1.15	0.613	8.831	0.000	معنوي
الفرضية الرئيسية	3.66	0.66	0.321	9.706	0.000	معنوي

اتضح من خلال الجدول رقم (15) الآتي:

الفرضية الرئيسية: وقد أظهرت النتائج في الجدول رقم (15) تبين أن متوسط الاستجابة (3.66) وهو أكبر من متوسط القياس (3) وأن الفروق تساوي (0.66) ولتحديد معنوية هذه الفروق فإن قيمة الدلالة الإحصائية تساوي أصغر من 0.05 وهذا يشير إلى أن هناك معنوية فروق عليا نقوم بقبول الفرض القائل (يؤثر تحليل الأمن السيبراني على حماية البيانات المالية الحساسة في نظم المعلومات المحاسبية محل الدراسة) حسب عينة الدراسة عند مستوى دلالة (0.05) وهذا يعتمد على تحليل الأمن السيبراني ضروري لحماية البيانات المالية الحساسة في نظم المعلومات المحاسبية، ويساعد المؤسسات المالية على تجنب المخاطر والحفاظ على ثقة العملاء.

- الفرضية الفرعية الأولى: وقد أظهرت النتائج في الجدول رقم (15) تبين أن متوسط الاستجابة (3.75) وهو أكبر من متوسط القياس (3) وأن الفروق تساوي (0.75) ولتحديد معنوية هذه الفروق فإن قيمة الدلالة الإحصائية تساوي أصغر من 0.05 وهذا يشير إلى أن هناك معنوية فروق عليا نقوم بقبول الفرض

القائل (تؤثر سياسات التحكم في الوصول على أمن البيانات المالية الحساسة) حسب عينة الدراسة عند مستوى دلالة (0.05)."

- الفرضية الفرعية الثانية: وقد أظهرت النتائج في الجدول رقم (15) تبين أن متوسط الاستجابة (3.08) وهو أكبر من متوسط القياس (3) وأن الفروق تساوي (0.08) ولتحديد معنوية هذه الفروق فإن قيمة الدلالة الإحصائية تساوي أكبر من 0.05 وهي 0.304 وهذا يشير إلى أن ليس هناك معنوية فروق عليا نقوم برفض الفرض البديل وقبول الفرض الصفري القائل (لا يتم تحديد وقياس فعالية استراتيجيات استجابة الحوادث عند حدوث خرق بيانات) حسب عينة الدراسة عند مستوى دلالة (0.05)."

- الفرضية الفرعية الثالثة: وقد أظهرت النتائج في الجدول رقم (15) تبين أن متوسط الاستجابة (4.15) وهو أكبر من متوسط القياس (3) وأن الفروق تساوي (1.15) ولتحديد معنوية هذه الفروق فإن قيمة الدلالة الإحصائية تساوي أصغر من 0.05 وهذا يشير إلى أن هناك معنوية فروق عليا نقوم بقبول الفرض القائل (يتم استخدام تحليل البيانات للكشف عن نقاط الضعف في نظم المعلومات المحاسبية) حسب عينة الدراسة عند مستوى دلالة (0.05)."

النتائج والتوصيات

1. النتائج:

- من خلال ما تقدم من دراسة ومن خلال التحليل الإحصائي، توصل الباحثان إلى النتائج التالية:
1. تبين من النتائج أنه يؤثر تحليل الأمن السيبراني على حماية البيانات المالية الحساسة في نظم المعلومات المحاسبية لدى عينة الدراسة.
 2. اتضح أنه تؤثر سياسات التحكم في الوصول على أمن البيانات المالية الحساسة.
 3. لا حظ أنه لا يتم تحديد وقياس فعالية استراتيجيات استجابة الحوادث عند حدوث خرق بيانات لدى مصنع أسمنت المرقب.
 4. تبين أنه يتم استخدام تحليل البيانات للكشف عن نقاط الضعف في نظم المعلومات المحاسبية.

2. التوصيات:

بناءً على نتائج البحث يوصي الباحثان بما يلي:

- يجب أن يتم تحديد وقياس فعالية استراتيجيات استجابة الحوادث عند حدوث خرق بيانات.
- تنظيم ورش عمل وبرامج تدريبية للموظفين حول أهمية تحليل الأمن السيبراني وتأثيره.
- أجري تقييم شامل للمخاطر السيبرانية التي تواجه نظم المعلومات المحاسبية في الشركات الصناعية. يُمكن استخدام أدوات تحليل المخاطر لتحديد الثغرات المحتملة.
- ضع سياسات واضحة لأمن المعلومات تشمل إجراءات التشفير، والتحكم في الوصول، والتعامل مع البيانات الحساسة.
- أعد خطط لاستجابة فورية في حال حدوث اختراق أو خرق للبيانات، بما يشمل التواصل مع الجهات المعنية وإصلاح الثغرات.
- تواصل مع شركات مختصة في مجال أمن المعلومات للحصول على استشارات مهنية وتحديثات حول أحدث التهديدات والحلول.
- ضع آلية لمراجعة الأداء الدوري لنظم الأمن السيبراني وتحديد مجالات التحسين.

المراجع

أولاً: المراجع العربية:

- إيمان السيد محمد عبدالله، (2024). العلاقة بين تفعيل أدوات الأمن السيبراني وأنظمة محاسبة التكاليف الرقمية دراسة تطبيقية على شركات القطاع العقاري بمصر، المجلة العلمية للبحوث والدراسات التجارية المجلد 38 - العدد الأول -2024، جامعة حلوان، كلية التجارة وإدارة الأعمال.
- دراسة (عبد السلام عطية عبد السلام يوسف، 2024، بعنوان (تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية الليبية: دراسة وصفية) المجلة العلمية للدراسات التجارية والبيئية، المجلد 15 - العدد الأول - 2024، جامعة قناة السويس (فرع الاسماعيلية)، مكتبة كلية التجارة.

- دراسة (2022, Daoud, & Serag) بعنوان "إطار مقترح لدراسة تأثير الأمن السيبراني على المعلومات المحاسبية لزيادة الثقة في التقارير المالية في سياق الصناعة 4.0: مدخل للحدث والأثر والاستجابة.
- دراسة (السرطان وآخرون، 2020 م) بعنوان "أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية في البنوك التجارية الأردنية، جامعة آل البيت، كلية الاقتصاد والعلوم الإدارية.
- النجار، فايز جمعة؛ النجار، نبيل جمعه؛ الزعبي، ماجد راضي، (2020): أساليب البحث العلمي: منظور تطبيقي، الطبعة الخامسة، دار الحامد للنشر والتوزيع، عمان، الأردن.
- محمود، سوميه شكري محمد، (2019): الأخطاء الشائعة في إجراءات التحقق من ثبات وصدق أدوات القياس المستخدمة في البحوث التربوية العربية، مجلة التربية للبحوث والنشر العلمي، العدد (7)، المجلد (35)، جامعة أسيوط، أسيوط، مصر.
- الهيئة الوطنية لأمن السيبراني بالمملكة العربية السعودية (2018) "تعريف الأمن السيبراني". الحساب الرسمي للهيئة على موقع التواصل الاجتماعي "تويتر. الرابط:
https://twitter.com/NCA_KSA/status/1023917241870557184
- النعيمي، محمد عبد العال؛ خليفة، غازي جمال؛ البياتي، عبد الجبار توفيق، (2015): طرق ومناهج البحث العلمي، الطبعة الأولى، مؤسسة الوراق للنشر والتوزيع، عمان، الأردن.
- عبيدات، ذوقان؛ كايد، عبد الحق؛ رزق، عبد الرحمن، (2015): البحث العلمي: مفهومه وأدواته وأساليبه، الطبعة السابعة عشر، دار الفكر ناشرون موزعون، عمان، الأردن.
- العساف، صالح بن حمد، (2014): المدخل إلى البحث في العلوم السلوكية، دار الزهراء للنشر والتوزيع، الرياض، المملكة العربية السعودية.

ثانياً: المراجع الأجنبية:

- Netemeyer, R. G., Bearden, W. O., & Sharma, S. (2003). Scaling Procedures: Issues and Applications. Thousand Oaks, CA: Sage Publications.
- Saunders, M. N., Lewis, P., & Thornhill, A. (2009). Research Methods for Business Students (5th Edition). London, United Kingdom: Pearson Education.

-
- Linthicum, S. (2010), "Cloud Computing and SOA Convergence in your Enterprise", Pearson Education, USA, pp.1-54.
 - Khanom, T. (2017), "Cloud Accounting: A Theoretical Overview", Journal of Business and Management, Vol.19, No.6, PP.31-38