جمهورية مصر العربية

معهد التخطيط القومي

الدراسات العليا

البحث التطبيقي

عنوان البحث باللغة العربية	تقييم فاعلية الإجراءات الوقائية ضد مخاطر الأمن السيبراني – بالشركات التكنولوجيه الصغيرة والمتوسطة بالقاهره
عنوان البحث باللغة الإنجليزية	**Evaluation of the Effectiveness of Preventive Measures Against Cybersecurity Risks in Small and Medium-Sized Technology Enterprises in Cairo**
إعداد	الباحث (مهندس) / اشرف عبداللاه ابراهيم
إشراف	أ.د بسمه محرم الحداد استاذ تكنولوجيا المعلومات والحاسبات والذكاء الاصطناعي بمعهد التخطيط القومي مدير مركز الأساليب التخطيطيه بالمعهد

لاستكمال متطلبات

الحصول على الماجستير المهني "المتابعة والتقييم"

مايو 2026

فهرس المحتويات

الملخص

تناولت هذه الدراسة رصد واقع الامن السيبراني ومدي فعالية الاجراءات المتبعة في الشركات التكنولوجية الصغيرة والمتوسطة بمدينة القاهرة. فقد انطلقت الدراسه من إشكالية أن هذه الشركات تشكل الحلقة الأضعف في سلاسل التوريد الرقمية بسبب محدودية الموارد وعدم الامتثال القانوني ووجود فجوة بين إدراك المخاطر نظرياً وترجمتها إلى ممارسات أمنية حقيقة.

واعتمدت الدراسة على المنهج الوصفي التحليلي التطبيقي، من خلال دراسة شملت عينة قوامها 30 شركة تعمل بمجال التكنولوجيا الرقميه في القاهرة. وقد استخدمت أدوات الاستبانة والمقابلات لجمع البيانات وتحليل الفجوات بين الواقع العملي والمتطلبات المعيارية الدولية.

حيث أظهرت النتائج وجود قصور إجرائي واضح ناتج عن غياب الموارد المالية والبشرية المخصصة للأمن السيبراني وتجاهل الامتثال القانوني مما يعرض هذه الشركات لمخاطر سيبرانية مرتفعة. وفي ضوء ذلك، قدمت الدراسة إطاراً مبدئيا عملياً مُصمماً خصيصاً للشركات الصغيرة والمتوسطة يجمع بين متطلبات قانون حماية البيانات المصري رقم 151 لسنة 2020 وضوابط المعايير الدولية المعتمدة.

وقد اوصت الدراسة بضرورة اصدار اعتماد مستندي للاجراءات الامنيه السيبرانيه للشركات من خلال منصة تفاعل رقميه تتبع الجهات المنظمة للأمن السيبراني (مرفق تنظيم الاتصالات) بمصر وتعتمد على الذكاء الاصطناعي لتبسيط عمليات التقييم والتدقيق ومنح شهادات الامتثال. كما أوصت بتخصيص نسبة لا تقل عن 1% من الميزانية السنوية لشركات الأمن السيبراني، وتفعيل برامج تدريب هجينة تركز على مهارات الحماية والاستجابة والتعافي، بهدف تحويل الأمن السيبراني من عبء مالي إلى ميزة تنافسية مستدامة تعزز ثقة العملاء واستمرارية الأعمال في السوق المصري.

الكلمات المفتاحية: الامن السيبراني، التهديدات السيبرانية، الشركات الصغيرة والمتوسطة.

Abstract

This study examined the reality of cybersecurity and the effectiveness of measures implemented within small and medium-sized technology enterprises (SMEs) in Cairo. The study originated from the problem that these companies constitute the weakest link in digital supply chains due to limited resources, lack of legal compliance, and the existence of a gap between theoretical risk perception and its translation into actual security practices. The study relied on the applied descriptive-analytical curriculum, through a study that included a sample of 30 companies operating in the field of digital technology in Cairo. It utilized questionnaires and interviews as tools for data collection and to analyze the gaps between practical reality and international standard requirements.

The results revealed a clear procedural deficiency resulting from the absence of financial and human resources dedicated to cybersecurity and the disregard for legal compliance, which exposes these companies to high cyber risks. In light of this, the study presented a preliminary practical framework specifically designed for SMEs that combines the requirements of the Egyptian Data Protection Law No. 151 of 2020 with approved international standards. The study recommended the necessity of issuing a documentary credit for the cybersecurity procedures of companies through a digital interaction platform affiliated with the cybersecurity regulatory authorities (National Telecommunications Regulatory Authority) in Egypt, relying on artificial intelligence to simplify assessment and auditing processes and grant compliance certificates. It also recommended allocating no less than 1% of the companies' annual budget to cybersecurity and activating hybrid training programs focusing on protection, response, and recovery skills, with the aim of transforming cybersecurity from a financial burden into a sustainable competitive advantage that enhances customer confidence and business continuity in the Egyptian market.

Keywords: Cybersecurity, Cyber Threats, Small and Medium-sized Enterprises (SMEs).

القسم الأول: الإطار العام للبحث

مقدمة البحث

تشير تقارير البنك الدولي والمنظمات الدولية المعنية بالتنمية إلى أن التحول الرقمي أصبح ضرورة ملحّة لتحقيق النمو الاقتصادي والتنمية البشرية، ولم يعد خيارًا قابلًا للتأجيل. وانطلاقًا من هذا الإدراك، تبنّت الدولة المصرية سياسة شاملة للتحول الرقمي باعتبارها ركيزة أساسية ضمن « رؤية مصر 2030»، بهدف تعزيز كفاءة الخدمات، ودعم التنافسية، وتحقيق التنمية المستدامة. وفي هذا السياق، أطلقت الدولة المصرية الاستراتيجية الوطنية للأمن السيبراني(2023–2027) ، وصدر القانون رقم 151 لسنة 2020 بشأن حماية البيانات الشخصية ليُشكّل إطارًا تشريعيًا ينظم عمليات جمع البيانات ومعالجتها وحمايتها.

ولأن الاقتصاد يمثل المحرك الرئيسي للتنمية، ويعتمد بدرجة كبيرة على نشاط القطاع الخاص إلى جانب الأنشطة الحكومية، تحتل الشركات الصغيرة والمتوسطة مكانة محورية في دعم التحول الرقمي، حيث تمثل الشركات الصغيرة والمتوسطة نحو (98%) من إجمالي المنشآت الخاصة وتوفر قرابة (80%) من فرص العمل وفقا لتقرير (OECD,2025). ويُعد قطاع تكنولوجيا المعلومات والاتصالات من أسرع القطاعات نموًا في مصر، بمساهمة بلغت (5.8%) من الناتج المحلي الإجمالي، ومعدل نمو سنوي تجاوز (17%) (Morder Intelligence,2025). وتواجه الشركات الصغيرة والمتوسطة في مصر تصاعدًا ملحوظًا في التهديدات السيبرانية خلال السنوات الأخيرة، حيث تشير التقارير إلى أن نحو (62%) من هذه الشركات تعرضت لهجمات إلكترونية عام 2024 (وزارة الاتصالات وتكنولوجيا المعلومات، 2024). وتعد هجمات الفدية والتصيد الإلكتروني أكثر الأنماط شيوعًا(Kaspersky,2024) . بينما لا تمتلك سوى (23%) من تلك الشركات خطة استجابة للحوادث الأمنية(Cisco,2023) . وقد صنّف تقرير (Kaspersky,2024) مصر ضمن الدول الأكثر استهدافًا في شمال إفريقيا. فيما أكد تقرير وزارة الاتصالات المصرية أن واحدة من كل ثلاث شركات صغيرة واجهت خرقًا أمنيًا فعليًا (وزارة الاتصالات وتكنولوجيا المعلومات، 2024). هذه المؤشرات تؤكد الحاجة الماسة إلى تعزيز الوعي والجاهزية الأمنية لدى هذا القطاع الحيوي الذي يمثل العمود الفقري للاقتصاد الوطني (مجلة الإسكندرية للبحوث الإدارية والاقتصادية، 2024). ورغم وجود إطار تشريعي وطني متمثل في قانون حماية البيانات الشخصية رقم 151 لسنة 2020. فإنه توجد فجوة محتملة بين المتطلبات القانونية والمعيارية من جهة، ومستوى تطبيق الإجراءات الوقائية داخل الشركات التكنولوجية الصغيرة والمتوسطة في القاهرة من جهة أخرى ومن هنا برزت أهمية هذا البحث الذي يهدف إلى **"تقييم فاعلية الإجراءات الوقائية ضد مخاطر الأمن السيبراني في الشركات التكنولوجية الصغيرة والمتوسطة بالقاهرة"**، من خلال قياس مستوى التزامها بالتشريعات الوطنية والمعايير الدولية، وتشخيص أوجه القصور والتحديات التي تواجهها، وصولًا إلى تقديم توصيات عملية وإطار تطبيقي قابل للتنفيذ يُسهم في تعزيز جاهزيتها الدفاعية وضمان استدامتها في بيئة رقمية سريعة التغيّر.

1.1 مشكلة البحث

تواجه الشركات الصغيرة والمتوسطة في مختلف أنحاء العالم تحديًا متزايدًا في مجال الأمن السيبراني، إذ أصبحت الهجمات السيبرانية أكثر تعقيدًا وتنوعًا، وتجمع بين أساليب تقليدية ومتطورة تعتمد على الأتمتة والذكاء الاصطناعي. وتشير التقارير الدولية الحديثة، وفي مقدمتها تقرير IBM Cost of a Data Breach Report 2025 ، إلى أن ما يقارب ثلاثة أرباع الهجمات السيبرانية تستهدف هذه الشركات، باعتبارها الحلقة الأضعف في سلاسل التوريد الرقمية. وقد بلغ متوسط التكلفة المالية لهذه الهجمات 2.8 مليون دولار أمريكي، وقد ترتفع إلى 4.88 مليون دولار في حالات الاختراقات الداخلية أو تلك التي

تؤثر على السمعة المؤسسية. وتزداد خطورة هذا الواقع عندما تكون هذه الشركات جزءًا من مشروعات قومية أو تقدم خدمات استراتيجية، مما يجعلها هدفًا جذابًا للمهاجمين رغم محدودية مواردها التقنية والبشرية. وفي هذا السياق، غالبًا ما تجد الشركات نفسها في موقف دفاعي كرد فعل للهجمات، وفي مواجهة مهاجمين يمتلكون زمام المبادرة والمفاجأة. أما في السياق المصري، فيتفاقم التحدي بسبب تأخر صدور اللائحة التنفيذية لقانون حماية البيانات الشخصية رقم 151 لسنة 2020، مما أدى إلى ضعف الإطار التنظيمي وتجاهل الالتزام بمتطلبات الأمن السيبراني. وبالتالي، تظل هذه الشركات عرضة لمخاطر سيبرانية مرتفعة نتيجة ضعف الإجراءات الوقائية والفجوة بين الوعي النظري والتطبيق العملي.وفي ضوء ما تقدم، تتمثل **مشكلة البحث** في الحاجة الملحة إلى **تقييم فاعلية الإجراءات الوقائية ضد مخاطر الامن السيبراني – بالشركات التكنولوجيه الصغيرة والمتوسطة بالقاهره** ، حيث تكون إجراءات الشركات ذو فعالية عندما تحقق الغرض المخصص لها وهي الاستعداد لمواجهة التهديدات السيبرانية وتقليل الاثار الناتجة من الاختراقات الأمنية السيبرانية وذلك من خلال قياس مدى تبنيها للمعايير الدولية مثل ISO/IEC 27001 ومدى التزامها بأحكام قانون حماية البيانات الشخصية رقم 151 لسنة 2020 في ظل غياب لائحته التنفيذية، مع تحديد أبرز الثغرات التقنية والتنظيمية والبشرية التي تزيد من تعرضها للهجمات السيبرانية.

1.2 أهداف البحث

يهدف هذا البحث إلى تقييم فاعلية الإجراءات الوقائية للأمن السيبراني داخل الشركات التكنولوجية الصغيرة والمتوسطة في مدينة القاهرة، من خلال تحليل مستوى جاهزيتها التنظيمية والتقنية والبشرية في مواجهة التهديدات السيبرانية المتزايدة والمتطورة. ويتحقق ذلك من خلال الأهداف الفرعية التالية:

- تحديد أبرز نقاط الضعف التقنية والتنظيمية والبشرية في هذه الشركات.
- قياس مدى وعي الشركات التكنولوجية الصغيرة والمتوسطة بالتشريعات الوطنية المنظمة للأمن السيبراني، وبخاصة قانون حماية البيانات الشخصية رقم 151 لسنة 2020.
- تحليل مدى تبنّي الشركات التكنولوجية الصغيرة والمتوسطة للمعايير والأطر الدولية للأمن السيبراني، وتقييم مدى توافق هذه المعايير مع إمكاناتها الواقعية.
- تقييم مدى ملاءمة الإجراءات الأمنية الحالية ومستوى الجاهزية السيبرانية الشاملة لهذه الشركات في ضوء نتائج القياس والتحليل.
- إعداد إطار عمل مبدئي مبسّط لتعزيز الأمن السيبراني داخل الشركات التكنولوجية الصغيرة والمتوسطة، بما يدعم جاهزيتها ويحسّن قدرتها على الامتثال للتشريعات والتصدي للتهديدات السيبرانية.
- الخروج بتوصيات عملية تهدف إلى تعزيز الأمن السيبراني للشركات الصغيرة والمتوسطة في ظل محدودية الموارد المتاحة.

1.3 أهمية البحث

يمكن إيجاز أهمية هذا البحث في بعدين رئيسيين، هما الأهمية النظرية والأهمية التطبيقية، وذلك على النحو الآتي:

أولًا: الأهمية النظرية للبحث

يساهم هذا البحث في إثراء الأدبيات العلمية المتعلقة بالأمن السيبراني في قطاع الشركات الصغيرة والمتوسطة، من خلال تقديم تحليل عميق لمستوى الوعي بالمخاطر السيبرانية وتأثيراتها الاقتصادية. كما يقدم وصفًا علميًا دقيقًا لواقع الممارسات الأمنية داخل الشركات التكنولوجية في القاهرة، وهو سياق لا يزال محدود الدراسة في الأدبيات العربية والمصرية. ويعمل

البحث على تقييم مدى ملاءمة الأطر والمعايير الدولية للبيئة المصرية، مما يساعد في سد فجوة معرفية مهمة ترتبط بالعلاقة بين الوعي السيبراني والجاهزية المؤسسية في السياق المحلي، ويفتح المجال أمام بحوث مستقبلية.

ثانيًا: الأهمية التطبيقية للبحث

يمتلك البحث أهمية تطبيقية مباشرة، إذ يقدم تقييمًا واقعيًا لمستوى جاهزية الشركات التكنولوجية الصغيرة والمتوسطة في القاهرة لمواجهة التهديدات السيبرانية، ويكشف نقاط الضعف التقنية والتنظيمية والبشرية. ويساعد نتائجه صانعي القرار والجهات الحكومية على وضع سياسات ومبادرات فعالة لدعم هذا القطاع الحيوي. كما يوجه الشركات نحو اختيار الأطر والمعايير الأنسب لبيئتها المحلية، ويقدم نموذجًا عمليًا مبسطًا لتقييم وتعزيز الأمن السيبراني. ومن خلال التوصيات العملية، يساهم البحث في رفع كفاءة العاملين ودعم جهود التحول الرقمي الآمن في مصر، مع تقليل المخاطر والخسائر المحتملة في ظل محدودية الموارد.

1.4 فروض أو تساؤلات البحث

السؤال الأول: ما أبرز نقاط الضعف التقنية والتنظيمية والبشرية التي تزيد من قابلية الشركات التكنولوجية الصغيرة والمتوسطة للتعرض للهجمات السيبرانية؟

السؤال الثاني: إلى أي مدى تلتزم الشركات التكنولوجية الصغيرة والمتوسطة بالتشريعات الوطنية المنظمة للأمن السيبراني، وبخاصة قانون حماية البيانات الشخصية رقم 151 لسنة 2020؟

السؤال الثالث: إلى أي مدى تتبنّى الشركات التكنولوجية الصغيرة والمتوسطة المعايير والأطر الدولية للأمن السيبراني، مثل ISO/IEC 27001وإطار NIST CSF ، وكيف يمكن تفسير مدى توافق هذه الأطر مع إمكاناتها الفعلية؟

السؤال الرابع: إلى أي مدى تعكس الإجراءات الأمنية المتبعة لدى الشركات التكنولوجية الصغيرة والمتوسطة مستوىً مناسبًا من الجاهزية السيبرانية لمواجهة الهجمات السيبرانية المتطورة؟

السؤال الخامس: ما الإطار العملي المقترح لتعزيز الأمن السيبراني داخل الشركات التكنولوجية الصغيرة والمتوسطة في القاهرة؟

1.5 حدود البحث

أولا : الحدود الموضوعية

يركّز هذا البحث على تقييم تأثير التهديدات السيبرانية على الشركات التكنولوجية الصغيرة والمتوسطة في محافظة القاهرة، وتحليل فاعلية الإجراءات الوقائية التي تتبنّاها هذه الشركات في حماية بنيتها الرقمية.

ثانيا: الحدود الزمنية

يعتمد البحث على تحليل البيانات والممارسات الأمنية خلال الفترة من عام 2020 إلى عام 2025.

ثالثا:الحدود المكانية

يقتصر البحث على الشركات التكنولوجية الصغيرة والمتوسطة في محافظة القاهرة فقط.

1.6 منهج البحث

تعتمد الدراسة على المنهج **الوصفي التحليلي التطبيقي** لتقييم واقع الأمن السيبراني وفاعلية الإجراءات الوقائية في الشركات الصغيرة والمتوسطة، مع اقتراح إطار عملي مطوَّر يتناسب مع إمكانياتها.

ويتكون المنهج من ثلاثة مستويات مترابطة:

- **المنهج الوصفي** :رصد وتوصيف واقع الأمن السيبراني والمخاطر التي تواجه الشركات.

-**المنهج التحليلي** :تحليل البيانات ودراسة الفجوة بين الممارسات الحالية والمعايير الدولية.

- **المنهج التطبيقي** :تطوير إطار عمل مقترح من خلال انتقاء وتطويع أفضل العناصر من الأطر الدولية (NIST CSF 2.0و ISO 27001) بما يناسب موارد الشركات الصغيرة والمتوسطة.

1.7 مصادر البيانات

هذا وسوف يعتمد البحث على مجموعة من مصادر البيانات المتنوعة لضمان شمولية ودقة التحليل

أولًا: البيانات الأولية (البحوث الميدانية)

تتمثل البيانات الأولية في المعلومات التي سيتم جمعها مباشرة من الشركات التكنولوجية الصغيرة والمتوسطة في محافظة القاهرة، وذلك باستخدام الأدوات التالية:

الاستبيانات(Questionnaires)

حيث توزَّع استبيانات على مديري الشركات والعاملين المرتبطين بالأمن السيبراني بهدف قياس مستوى الوعي بالتهديدات السيبرانية، ومدى تطبيق الإجراءات الوقائية، وجاهزية البنية التحتية الرقمية، وحجم الموارد المخصصة للوقاية والاستجابة للحوادث. وهذه البيانات تمثل الأساس الكمي للتحليل.

دراسات الحالة(Case Studies)

يتم تحليل حالات واقعية لاختراقات أو حوادث سيبرانية تعرّضت لها بعض هذة الشركات، بهدف فهم حجم الأضرار، وتقييم قدرة الشركات على التعامل مع الحادث، وتحليل تأثير الاختراق على العمليات التجارية وسلاسل التوريد.

ثانيًا: البيانات الثانوية(Secondary Data)

تمثل البيانات التي يتم جمعها من مصادر مكتبية ومنشورة، وتشمل:

التشريعات والقوانين المصرية الخاصة بالأمن السيبراني وتكنولوجيا المعلومات، وسياسات جهاز تنظيم الاتصالات.

والاحصاءات الوطنية والدولية حول أمن الشركات الصغيرة، وتقارير مؤسسات مثلITU ، WEF، NIST، Kaspersky، Cisco. التي تُستخدم لدعم التحليل وتفسير الاتجاهات الحديثة.

1.8 المفاهيم البحثية

جدول رقم 1 : المفاهيم البحثية

المصطلح البحثي	التعريف الإجرائي / الأكاديمي	المصدر
الأمن السيبراني (Cybersecurity)	مجموعة الممارسات والتقنيات والعمليات المصممة لحماية الشبكات والأجهزة والبرمجيات والبيانات من الهجمات أو الوصول غير المصرح به، مع ضمان تحقيق مثلث السرية والسلامة والتوافر (CIA Triad).	(NIST, 2023)
التهديدات السيبرانية (Cyber Threats)	أي ظرف أو حدث خبيث (بشري أو غير بشري) يملك القدرة على إحداث تأثير سلبي على الأصول التنظيمية من خلال استغلال ثغرة أمنية بقصد السرقة أو التعطيل أو التجسس.	(ENISA Threat Landscape, 2024)

المشروعات الصغيرة والمتوسطة (SMEs)	مؤسسات مسجلة يقل عدد العاملين فيها عادة عن 300 موظف، وتختلف في حجمها ونشاطها بناءً على معايير عدد العاملين، أو رأس المال العامل، أو الإيرادات السنوية.	(International Finance Corporation [IFC], 2012)
الإجراءات الوقائية (Preventive Measures)	مجموعة الضوابط الفنية والإدارية والبشرية التي تُطبق استباقياً لتقليل احتمالية وقوع الحادث الأمني، مثل سياسات كلمات المرور، التحديثات الدورية، وأنظمة الكشف عن الاختراق.	(NIST SP 800-53 Rev. 5, 2020)
الوعي الأمني (Cybersecurity Awareness)	مستوى المعرفة والسلوكيات التي يمتلكها الأفراد تجاه المخاطر السيبرانية، والقدرة على التعرف على الهجمات مثل التصيد الاحتيالي والإبلاغ الفوري عن الحوادث.	(ISO/IEC 27032:2023)
الجاهزية السيبرانية (Cyber Readiness)	قدرة المنظمة على تنفيذ الوظائف الست لإطار NIST 2.0 (حوكمة، تحديد، حماية، كشف، استجابة، استعادة) بكفاءة وسرعة لمنع الهجمات والتعافي منها.	(NIST Cybersecurity Framework v2.0, 2024)
الإطار التنظيمي للأمن السيبراني	مجموعة القوانين واللوائح الوطنية (مثل قانون 151 لسنة 2020) والمعايير الدولية (مثل ISO 27001) التي تنظم حماية البيانات والأنظمة الحيوية.	(NTRA, 2023)

1.9 الدراسات السابقة

- أكدت دراسة **(خشبة – الريس وآخرون ،2021)** بعنوان " الأبعاد التنموية والاستراتيجية للأمن السيبراني و دوره في دعم الاقتصاديات الرقمية والمشفرة مسارات التجربة المصرية فى ضوء التجارب العالمية" على الأهمية الاستراتيجية للأمن السيبراني كركيزة أساسية لدعم الاقتصاد الرقمي المصري وحماية منشآت الأعمال من التهديدات الإلكترونية المتزايدة. أوضحت الدراسة أن نجاح رؤية مصر 2030 يعتمد بشكل مباشر على بناء قدرات دفاعية قوية للقطاع الخاص، وخصّت الشركات الصغيرة والمتوسطة وريادة الأعمال بتركيز خاص لكونها العمود الفقري للاقتصاد المصري. أوصت بضرورة وضع إطار حوكمة شامل ومستدام يشمل جميع المنشآت، مع التعاون الوثيق مع جهاز تنمية المشروعات الصغيرة والمتوسطة، وتفعيل القانون رقم 151 لسنة 2020 بشأن حماية البيانات الشخصية كأداة تنظيمية مركزية.

- أجرت **(Bada , Nurse, 2021)** دراسة ميدانية موسعة شملت 312 موظفًا ومديرًا في شركات بريطانية صغيرة ومتوسطة لقياس فجوة الوعي الأمني. أظهرت النتائج أن 82% من المشاركين يمتلكون معرفة محدودة جدًا بأساليب الهجوم الحديثة مثل التصيّد الموجّه وبرمجيات الفدية، وأن 69% من الحوادث المسجلة كانت بسبب نقر الموظفين على روابط أو مرفقات خبيثة. أكدت الدراسة أن الشركات الصغيرة تفتقر لبرامج تدريب دورية وتعتمد فقط على مضادات فيروسات تقليدية، مما يجعلها فريسة سهلة. أوصى الباحثان بتطبيق برامج تدريب تفاعلية تحاكي هجمات حقيقية، وإنشاء ثقافة "الإبلاغ بدون خوف"، وتفعيل المصادقة متعددة العوامل كحد أدنى. تُعد هذه الدراسة من أقوى المراجع التي تثبت أن العامل البشري هو الحلقة الأضعف والأقوى في آن واحد.

- تناولت دراسة **(إبراهيم، يوسف وعيد ،2022)** مفهوم "النظافة الرقمية" كأحد أهم المرتكزات غير التقنية لتعزيز الأمن السيبراني داخل المؤسسات المصرية. اعتمد الباحثون منهجًا وصفيًا تحليليًا من خلال مراجعة شاملة للأدبيات وتحليل سلوكيات العاملين في 42 مؤسسة مصرية متنوعة الحجم. أثبتت النتائج أن 78% من الحوادث السيبرانية في الشركات الصغيرة والمتوسطة ناتجة عن أخطاء بشرية بسيطة يمكن تجنبها عبر ممارسات يومية رخيصة مثل تحديث البرمجيات، استخدام كلمات مرور قوية، تجنب الروابط المشبوهة، والإبلاغ الفوري عن الرسائل المريبة. أكدت الدراسة أن تنفيذ برامج توعية مستمرة وتدريبات قصيرة دورية يمكن أن يقلل معدل الحوادث بنسبة تصل إلى 65% دون تكلفة مادية كبيرة. خلصت إلى أن دمج النظافة الرقمية ضمن الثقافة التنظيمية هو الحل الأكثر فعالية من حيث التكلفة للشركات محدودة الموارد، لكنها تقيس العلاقة بين هذه الممارسات ومتطلبات القانون 151 بشكل مباشر.

- أجرت **(Erdogan , 2023)** دراسة بعنوان "Cybersecurity awareness and capacities of SMEs" بحثًا ميدانيًا شاملاً شمل 185 شركة صغيرة ومتوسطة من قطاعات متنوعة (تكنولوجيا، تجارة إلكترونية، خدمات). اعتمد الباحث منهجًا كميًا وصفيًا من خلال استبيان إلكتروني موجه لمديري الشركات ومسؤولي تكنولوجيا المعلومات، بالإضافة إلى 28 مقابلة شبه مهيكلة لتعميق النتائج. أظهرت الدراسة أن 71% من الشركات لا تطبق المصادقة متعددة العوامل MFA، و63% لا تمتلك خطة استجابة للحوادثIncident Response Plan ، وأن 58% فقط من الموظفين تلقوا تدريبًا أمنيًا في آخر عامين. كما كشفت أن 69% من مدراء الشركات الصغيرة يعتبرون الأمن السيبراني "تكلفة إضافية" وليس استثمارًا استراتيجيًا، وهو ما يفسر غياب الميزانيات المخصصة .أكدت الدراسة أن محدودية الميزانية ونقص الكفاءات المتخصصة يشكلان الحاجزين الأساسيين أمام بناء منظومة أمنية فعالة، حيث يعمل 82% من الشركات بموظف IT واحد أو بدون موظف متخصص أصلاً. من أبرز النتائج أيضًا أن 74% من الحوادث المسجلة كانت بسبب خطأ بشري يمكن تجنبه بتدريب بسيط.

- **وفي دراسة محدثه بواسطة (Tam,Rao,Hall ,2024) بعنوان** "The good, the bad and the missing: A narrative review of cyber-security implications for Australian small businesses"، تركز على الشركات الصغيرة جدًا (micro-businesses: 0–19 موظفًا). اعتمد الباحثون منهج المراجعة السردية Narrative Review من خلال تحليل أكثر من 180 مصدرًا (أكاديمي، حكومي، صناعي) لرسم صورة كاملة عن الواقع الأمني لهذه الفئة. أظهرت الدراسة أن الشركات الصغيرة أصبحت بعد جائحة كورونا هدفًا رئيسيًا للهجمات بسبب التحول السريع للعمل عن بُعد والتجارة الإلكترونية دون بناء دفاعات موازية .أبرزت الدراسة وجود فجوة بحثية خطيرة: معظم الدراسات تُدمج الشركات الصغيرة جدًا ضمن فئة SMEs العامة، مما يؤدي إلى نتائج غير دقيقة وغير قابلة للتطبيق على micro-businessesالتي تفتقر حتى لموظف IT بدوام كامل. كما كشفت عن تحديات بنيوية: نقص البيانات الفعلية عن الحوادث (بسبب عدم الإبلاغ)، ضعف الوعي، صعوبة تطبيق الأطر التقليدية، مشكلات قانونية في المساءلة، وقلة فعالية التأمين السيبراني لهذه الفئة .في المقابل، حددت الدراسة فرصًا ذهبية يمكن استغلالها بسبب صغر الحجم: (1) سرعة اتخاذ القرار وإمكانية تطبيق Zero Trust بسهولة، (2) الاستفادة من أدوات مفتوحة المصدر رخيصة، (3) إمكانية إنشاء تحالفات محلية بين الشركات الصغيرة لتبادل التهديدات والحلول، (4) مرونة كبيرة في التكيف مقارنة بالشركات الكبرى. خلصت الدراسة إلى أن معالجة الفجوات البحثية وتطوير نماذج دفاع مخصصة للشركات الصغيرة جدًا سيُحقق وفرًا اقتصاديًا كبيرًا ويقلل الخسائر المجتمعية الناتجة عن الهجمات. أوصى الباحثون بإنشاء مراكز دعم حكومية تقدم أدوات

مجانية وتدريب مبسط، وتطوير إطار "Cybersecurity-in-a-Box" خاص بال.micro-businesses تُعد هذه الدراسة من أقوى المراجع التي تُبرز الفرق الجوهري بين SMEs والmicro-businesses وتفتح الباب لأبحاث مستقبلية مخصصة.

- تناولت دراسة **(Hoong & Rezania, 2024)** إشكالية تحقيق التوازن بين العنصر البشري (المواهب والمهارات والحلول التكنولوجية في إدارة قضايا الأمن السيبراني وحماية الخصوصية داخل الشركات الصغيرة والمتوسطة(SMEs) ، في ظل تصاعد التهديدات الرقمية وتزايد المتطلبات التنظيمية. هدفت الدراسة إلى تحليل الكيفية التي تعتمد بها هذه الشركات على مزيج من القدرات البشرية والتقنية لمواجهة المخاطر السيبرانية، مع التركيز على القيود التي تواجهها من حيث الموارد المالية والبشرية. اعتمدت الدراسة على منهج نوعي تحليلي، حيث أجرى الباحثان مقابلات شبه مهيكلة مع مديري شركات صغيرة ومتوسطة ومسؤولي تقنية المعلومات، إضافة إلى تحليل ممارسات وسياسات الأمن السيبراني المطبقة داخل هذه الشركات. وركزت الدراسة على فهم القرارات الإدارية المتعلقة بالاستثمار في التكنولوجيا مقابل الاستثمار في تنمية مهارات العاملين، ومدى تأثير ذلك على فاعلية الإجراءات الوقائية. وأظهرت نتائج الدراسة أن الشركات الصغيرة والمتوسطة تميل غالبًا إلى الاعتماد على حلول تقنية جاهزة مثل البرمجيات الأمنية والخدمات السحابية، في مقابل إهمال نسبي لتطوير المهارات السيبرانية لدى العاملين. كما بيّنت النتائج أن هذا الاعتماد غير المتوازن يؤدي إلى ضعف القدرة على التعامل مع التهديدات المرتبطة بالهندسة الاجتماعية والتصيد الإلكتروني، حيث يظل العامل البشري الحلقة الأضعف في منظومة الحماية. وأكدت الدراسة أن نقص الكفاءات المتخصصة وارتفاع تكلفة توظيف خبراء الأمن السيبراني يمثلان عائقين رئيسيين أمام تحقيق مستوى نضج أمني متكامل. وخلصت الدراسة إلى أن فاعلية الأمن السيبراني في الشركات الصغيرة والمتوسطة تتطلب **نهجًا متوازنًا** يجمع بين الاستثمار في التكنولوجيا المناسبة وبناء القدرات البشرية من خلال التدريب والتوعية المستمرة. وأوصت بضرورة تبني سياسات أمنية مرنة، وتطوير ثقافة مؤسسية داعمة للأمن السيبراني، بما يسهم في تعزيز حماية البيانات والخصوصية وتقليل المخاطر السيبرانية.

- وأفاد (**Calvo,Manzano , 2025**) في دراسة بعنوان (CyberESP: An Integrated cybersecurity framework for SMEs) – تهدف إلى تطوير إطار متكامل للأمن السيبراني مخصّص خصيصًا للشركات الصغيرة والمتوسطة في ظل محدودية مواردها البشرية والتقنية والمالية. اعتمد الباحثون منهج البحث العلمي التصميمي Design Science Research Methodology (DSR)، وهو منهج يركز على بناء حلول عملية قابلة للتطبيق لحل مشكلات واقعية من خلال تصميم نموذج أولي، تقييمه، وتحسينه بشكل تكراري. بدأت الدراسة بتحليل معمق للأطر التقليدية الثقيلة مثل NIST Cybersecurity Framework و ISO/IEC 27001، وأظهرت أن هذه الأطر غير مناسبة لل SMEs بسبب تعقيدها، تكلفتها العالية، وافتقارها إلى الأتمتة، مما يجعل تطبيقها شبه مستحيل بدون استشاريين متخصصين .بناءً على ذلك، حدد الباحثون ستة متطلبات أساسية يجب أن يحققها أي إطار فعال للشركات الصغيرة: (1) إدارة الأصول الرقمية، (2) تحليل الثغرات الأمنية، (3) تحليل التهديدات، (4) تقييم المخاطر، (5) سهولة الاستخدام، (6) الأتمتة والتكامل.

- ونشر **(Al-Khasawneh, 2025)** دراسة بعنوان "The Role of Digital Transformation Capabilities in Improving Banking Performance in Jordanian Commercial Banks"، وإن كانت في القطاع المصرفي إلا أن نتائجها قابلة للتعميم على الشركات التكنولوجية الصغيرة في المنطقة العربية. استخدم الباحثون منهجًا مختلطًا (كمي

وكيفي) شمل استبيانات لـ 312 موظفًا ومقابلات مع 28 مديرًا تنفيذيًا. أظهرت النتائج أن القدرات الرقمية (البنية التحتية، الكفاءات البشرية، الثقافة التنظيمية) تُحسن الأداء المالي بنسبة 41%، لكن الأمن السيبراني يُعد العامل الأكثر تأثيرًا سلبيًا عند ضعفه .حددت الدراسة أن الشركات العربية (بما فيها الصغيرة) تعاني من ثغرات في الامتثال لقوانين حماية البيانات، ضعف الاستثمار في الحلول الأمنية المتقدمة، ونقص الكفاءات المتخصصة. أكد الباحثون أن التحول الرقمي بدون استراتيجية أمنية موازية يزيد المخاطر بنسبة 67%. قدموا نموذجًا مقترحًا يدمج الأمن السيبراني كركيزة أساسية ضمن قدرات التحول الرقمي، مع توصيات عملية: (1) تبني نهج "Security-by-Design" من البداية، (2) الاستثمار في تدريب الموظفين على التهديدات الحديثة، (3) التعاون مع مزودي خدمات سحابية معتمدين محليًا، (4) تطبيق إطار حوكمة أمنية بسيط يتناسب مع القوانين العربية المشابهة لقانون 151 المصري. تُعد هذه الدراسة مهمة لأنها الأولى في المنطقة العربية التي تربط بين التحول الرقمي والأداء مع إعطاء الأمن السيبراني وزناً إحصائياً واضحاً.

- تناولت دراسة (**Mkhulisi, 2025**) متطلبات المهارات السيبرانية اللازمة للعاملين في الشركات الصغيرة والمتوسطة، في ظل تصاعد التهديدات السيبرانية واعتماد هذه الشركات المتزايد على النظم الرقمية دون امتلاك بنية أمنية متخصصة. هدفت الدراسة إلى تحديد الفجوة بين المهارات المتوافرة لدى الموظفين ومتطلبات الحماية الفعّالة من المخاطر السيبرانية. واعتمد الباحث على المنهج الوصفي–التحليلي مدعومًا بأسلوب بحث نوعي من خلال إجراء مقابلات شبه مهيكلة مع موظفين ومديري تقنية المعلومات في عدد من الشركات الصغيرة والمتوسطة، إضافة إلى تحليل السياسات والإجراءات الأمنية المتبعة داخل هذه المؤسسات. أظهرت نتائج الدراسة أن غالبية الشركات الصغيرة والمتوسطة تعاني من ضعف واضح في المهارات السيبرانية لدى العاملين، خاصة فيما يتعلق بالتعرف على هجمات التصيّد الإلكتروني، وإدارة كلمات المرور، والاستجابة الأولية للحوادث، وحماية البيانات الحساسة. كما بيّنت النتائج أن العامل البشري يمثل أحد أهم أسباب نجاح الهجمات السيبرانية داخل هذه الشركات، نتيجة غياب التدريب المنتظم وضعف الثقافة الأمنية المؤسسية. وأكدت الدراسة أن الاعتماد على الحلول التقنية وحدها لا يكفي دون تعزيز قدرات العاملين. وأوصت بضرورة تبنّي برامج تدريب سيبراني مستمرة، ووضع سياسات واضحة، وربط تنمية المهارات السيبرانية بثقافة العمل داخل الشركات الصغيرة والمتوسطة كإجراء وقائي أساسي للحد من المخاطر السيبرانية.

- كذلك نشرت (**IBM Security**) تقريرها السنوي (IBM Cost of a Data Breach,2025) ، وهو أكبر تقرير عالمي من نوعه يعتمد على تحليل 604 منظمات في 16 دولة و17 قطاعًا. أظهر التقرير أن متوسط تكلفة الاختراق الواحد في 2025 بلغ 4.88 مليون دولار عالميًا، لكن الشركات الصغيرة والمتوسطة (أقل من 1000 موظف) سجلت متوسط تكلفة 2.9 مليون دولار – وهو رقم مدمر لشركة صغيرة. كشف التقرير أن 53% من الاختراقات جاءت عبر طرف ثالث (مورد أو شريك) ضعيف الحماية، وأن هجمات الفدية وسرقة بيانات الاعتماد شكلت 71% من الحوادث .ومن أقوى النتائج التي أشار اليها ان الشركات التي طبقت بنيةZero Trust قللت الخسائر بنسبة 42%، والتي نفذت تدريبًا دوريًا للموظفين وفرت 58% من التكلفة، بينما الشركات التي لا تملك فريق استجابة للحوادث دفعت 60% أكثر. أكد التقرير أن الشركات الصغيرة تستغرق 287 يومًا في المتوسط لاكتشاف الاختراق واكتشاف تأثيره – وهي فترة كافية لإفلاسها. قدم التقرير 8 توصيات أساسية للشركات الصغيرة أهمها: استخدام أدوات كشف مدعومة بالذكاء الاصطناعي، تفعيلMFA ، تقييم أمني دوري للموردين، ووضع خطة استجابة مكتوبة. يُعد هذا التقرير دليلاً قاطعًا على أن الاستثمار الوقائي البسيط يوفر ملايين الدولارات .

1.10 الفجوة البحثية

رغم الثراء في الدراسات السابقة، إلا أنها تكشف فجوة بحثية واضحة تتمثل في عدم وجود دراسات ميدانية تجريبية تركز على تقييم فاعلية الإجراءات الوقائية الفعلية في الشركات التكنولوجية الصغيرة بالقاهرة، مع قياس مدى الامتثال لقانون حماية البيانات الشخصية رقم 151 لسنة 2020. معظم الدراسات إما أو تركز على الوعي والتهديدات دون تقييم عملي للإجراءات، أو غير محلية (مثل الدراسات الأوروبية والأسترالية). كما لم تدمج أي دراسة بين السياق المصري والقانوني مع تقييم ميداني كمي–كيفي لأوجه القصور. **لذا تأتي الدراسة الحالية لسد هذه الفجوة من خلال تقييم ميداني دقيق للواقع، مع تقديم توصيات عملية مخصصة للبيئة المصرية، مما يعزز الاستدامة الرقمية للشركات التكنولوجية الصغيرة.**

القسم الثاني: الإطار النظري للبحث

المبحث الأول: مفاهيم وتحديات الامن السيبراني في ظل الأطر الدولية

2.1- مفهوم المجتمع الرقمي والتهديدات السيبرانية

يمثل المجتمع الرقمي في سياق الشركات الصغيرة والمتوسطة تحولاً بنيوياً أساسياً في البنية التحتية للمؤسسة، إذ لا يقتصر على مجرد استخدام الحواسيب، بل يعني الاندماج الكامل بين المكونات الرقمية والعمليات التشغيلية اليومية. ويتكون هذا المجتمع من ثلاثة محاور تقنية رئيسية تشكل البنية التحتية المعلوماتية:

أولاً: **المكونات المادية (Hardware)** التي تشمل محطات العمل والخوادم المحلية وأجهزة الشبكات الداخلية التي تضمن تدفق البيانات بين الأقسام.

وثانياً: **الأصول البرمجية (Software Assets)** التي تمتد من أنظمة التشغيل إلى برمجيات تخطيط موارد المنشأة (ERP) وقواعد البيانات المحلية التي تحفظ الأسرار التجارية والمالية.

ثالثاً:**الأصول البيانية (Data Assets)** التي تمثل النتاج الرقمي الحقيقي لقيمة المؤسسة، وتشمل ملفات المشاريع وبيانات العملاء والسجلات المحاسبية.

وفي ظل الاعتماد الكامل للشركات علي البيئه الرقميه في جميع اعمالها اليوميه وهي السبيل الوحيد للتواصل مع الجهات والشركات الاخرى فقد تحول مفهوم **التهديدات السيبرانية** من مجرد مشكلات تقنية تستهدف البنيه الرقميه إلى أدوات تعطيل موجهة ذات اغراض مختلفه سواء استراتيجية او ماليه او علميه ليس بالضروره تهدف الي تعطيل المنظومه الرقميه ولكن للحصول علي اقصي استفاده ممكنه. ويمكن ان تكون سلسلة من التهديدات المتتالية لإجبار الاهداف الي اتخاذ ردود الافعال المخطط لها.

2.2- انواع الهجمات السيبرانية وأنماط الاستهداف

يُعرف الهجوم السيبراني أكاديمياً بأنه أي محاولة غير مصرح بها للوصول إلى بيانات نظام المعلومات، أو تعطيله، أو تعديله، أو تدميره. ويمكن تصنيف الهجمات حسب طبيعة ونمط الاستهداف كالتالي:

جدول رقم 2 : مفاهيم الامن السيبراني

التصنيف (حسب CIA Triad)	نوع الهجوم	آلية التنفيذ (Mechanism)	الأثر الأكاديمي والبحثي
أولاً: هجمات التوافر (Availability)	حجب الخدمة الموزعة (DDoS)	إغراق موارد النظام بفيض من الطلبات الوهمية عبر شبكات (Botnets).	شلل العمليات التشغيلية، خسائر مالية، وفقدان الثقة بسبب خرق اتفاقيات الخدمة.
	برمجيات الفدية (Ransomware)	تشفير ملفات النظام وقواعد البيانات والمطالبة بفدية لفك التشفير.	تهديد مزدوج يضرب "التوافر" و"السرية"، ويمثل الخطر الأكبر على استدامة الشركات الصغيرة.
ثانياً: هجمات السرية (Confidentiality)	حقن التعليمات (SQL Injection)	استغلال ثغرات مدخلات المواقع لحقن أوامر تجبر قواعد البيانات على كشف محتواها.	المصدر الرئيسي لتسريب البيانات الضخمة، ووضع المؤسسة في مواجهة قانونية (قانون 151).
	الصيد الاحتيالي (Phishing)	استخدام الهندسة الاجتماعية لخداع الموظفين والحصول على بيانات الدخول.	يبرز أهمية "المحور البشري" وثغرات السلوك الفردي كحلقة أضعف في المنظومة الأمنية.
ثالثاً: هجمات السلامة (Integrity)	رجل في المنتصف (MitM)	اعتراض حركة البيانات بين طرفين والتجسس عليها أو تعديل محتواها سراً.	ضرب موثوقية الاتصالات، والتأكيد على ضرورة التشفير الشامل (End-to-End).
	تغيير واجهة المواقع (Defacement)	الدخول غير المصرح به لتعديل المحتوى البصري والرسائل في موقع الشركة.	أثر كارثي على سمعة المؤسسة وموثوقية علامتها التجارية أمام العملاء والمستثمرين.
رابعاً: الأنماط الحديثة (Supply Chain)	سلاسل التوريد الرقمية	زرع برمجيات خبيثة في تحديثات الموردين التقنيين للوصول لعملائهم.	فرض مراجعة سياسات "الثقة الصفرية" (Zero Trust) وإدارة مخاطر الطرف الثالث.
	الثغرات الصفرية (Zero-Day)	استهداف ثغرات برمجية غير معروفة للمطورين ولا توجد لها حلول دفاعية.	قمة التحدي السيبراني؛ تتطلب أنظمة كشف قائمة على "السلوك" لا "البصمة التقنية".

2.3- مفهوم الامن السيبراني ومخاطر الامن السيبراني وعلاقتها بالأطر الدولية

2.3.1- مفهوم الامن السيبراني

وفقا للتطور السريع الذي تشهده التهديدات السيبرانية فإن كمفهوم الامن السيبراني شهد تطور يتناسب مع ذلك فتجاوز مفهوم الحماية التقنية البحتة الي ان يصبح إطار متكامل يجمع بين الحوكمة والسياسات والإجراءات الدفاعية لحماية الفضاء السيبراني

(Cyberspace). ويشمل ذلك تأمين المكونات المادية(Hardware) ، والبرمجيات(Software) ، والبيانات، وقنوات الاتصال والشبكات التي تربط بينها، بالإضافة إلى السياسات والضوابط التنظيمية المنظمة لهذه العناصر، وذلك للحيلولة دون النفاذ غير المصرح به، أو التخريب، أو الاستغلال غير المشروع.

ويعتمد اي اطار للأمن السيبراني في جوهره على **نموذج الأبعاد الثلاثة(The CIA Triad)** ، والذي يُعد المرجع العالمي الأساسي لتقييم فعالية المنظومات الأمنية طبقا ل (NIST,2017)، فهو يتكون من:

- **السرية(Confidentiality)** : وتعني ضمان تقييد الوصول إلى المعلومات الحساسة للأطراف المخولة فقط، من خلال التشفير وآليات التحكم في الهوية الرقمية.
- **السلامة(Integrity)** :تعني الحفاظ على دقة البيانات وموثوقيتها، ومنع أي تعديل غير مصرح به، سواء كان متعمداً أو ناتجاً عن أخطاء تقنية.

التوافر(Availability) :تعني ضمان استمرارية عمل الأنظمة وإتاحة البيانات والخدمات عند الحاجة، مع تعزيز مقاومة البنية التحتية للهجمات والأعطال

2.3.2- مخاطر الامن السيبراني

وفقاً لـ(NIST SP 800-30 Rev. 1, 2012) National Institute of Standards and Technology ، يُعرف خطر الأمن السيبراني بأنه مقياس لمدى تعرض المنظمة لظرف أو حدث محتمل يؤدي إلى ضرر أو خسارة، ناتج عن استغلال الضعف في الأنظمة أو العمليات أو البشر. وتمثل هذه المخاطر الجانب المقابل للأمن السيبراني، إذ إنها تهدد الركائز الثلاثة الأساسية لأمن المعلومات، وهي :**السرية(Confidentiality)** ، **السلامة(Integrity)** ، و**التوافر (Availability)**. وقد تؤدي هذه المخاطر في نهاية المطاف إلى أضرار مالية، تشغيلية، قانونية، أو سمعية، وقد تصل إلى الشلل التشغيلي أو الاستراتيجي للشركات، خاصة الصغيرة والمتوسطة.

ويمكن تناول مخاطر الأمن السيبراني من خلال منظورين متكاملين:

المنظور الأول: المنظور التقني والتشغيلي يركز على المكونات المباشرة للمخاطر، ويشمل التهديدات(Threats) ، والثغرات(Vulnerabilities) ، والتأثيرات المحتملة .(Impacts) ويهدف هذا المنظور إلى تحديد الضعف الفني والإجرائي والبشري، وتقييم احتمالية حدوث الهجمات وشدة تأثيرها على الأنظمة والشبكات.

المنظور الثاني: المنظور الاستراتيجي والتجاري يركز على الآثار الأوسع للمخاطر على مستوى المنشأة ككل، مثل التأثير على استمرارية الأعمال، والخسائر المالية، والالتزامات القانونية والتنظيمية، والسمعة التجارية، وثقة العملاء. ويهدف هذا المنظور إلى ربط المخاطر السيبرانية بأهداف المنظمة الاستراتيجية وقياسها من منظور الأعمال.

2.3.3- الأطر والمعايير الدولية لتعزيز الامن السيبراني

المعايير الدولية هي المسطرة التي تحول الأمن السيبراني من حالة شعورية إلى قيمة رقمية قابلة للقياس – ففي ظل التطور المتسارع للتهديدات السيبرانية وتعقيد البنية التكنولوجية للمؤسسات، لم يعد تأمين الأصول الرقمية مجرد خيار تقني يعتمد على اجتهادات فردية، بل أضحى ضرورة استراتيجية تتطلب أطراً مرجعية موحدة. ومن أجل بناء رؤية علمية لتقييم فاعلية الإجراءات الوقائية، يستوجب الأمر التمييز بين مفهومين جوهريين يشكلان حجر الزاوية في حوكمة الأمن الرقمي:

أولاً: إطار العمل (Framework) : وهو الوعاء الهيكلي والمرن الذي يحدد "كيفية التفكير "في إدارة الأمن السيبراني. فهو يمثل خارطة طريق استراتيجية توفر لغة مشتركة بين الإدارة العليا والفرق الفنية، ويتميز بكونه توجيها يمنح الشركات مساحة

لتكييف عناصره بما يتناسب مع حجم مخاطرها ومواردها المتاحة، مما يجعله بمثابة "البوصلة التي توجّه جهود الأمن السيبراني نحو تحقيق الصمود الرقمي.

ثانياً: المعايير :(Standards) وهي الجانب الإلزامي والقياسي الذي يحدد ما يجب القيام به بدقة متناهية. تُمثل المعايير المسطرة الفنية والنوعية التي لا تقبل التأويل، وتهدف إلى توحيد جودة الممارسات الأمنية. وبخلاف أطر العمل، تتسم المعايير بكونها قابلة للقياس والتدقيق(Auditable) ، حيث تُستخدم كمرجع أساسي للحصول على الشهادات الدولية أو لإثبات الامتثال القانوني، فهي تمثل الحد الأدنى من الجودة التقنية والإدارية اللازمة لضمان سلامة الأصول المعلوماتية

لذلك فان المعيار الدولي هو وثيقة فنية وإدارية يتم وضعها بالإجماع وتعتمدها جهة معترف بها عالمياً (مثل منظمة ISO). هي اتفاقية جودة "تحدد القواعد، الخطوط التوجيهية، أو الخصائص اللازمة لضمان أن العمليات والخدمات والأنظمة التكنولوجية تعمل بكفاءة، وأمان، وقابلية للتوافق مع الأنظمة الأخرى.

وتتعدد الأمثلة حسب زاوية التركيز، ومن أبرزها:

- **ISO/IEC 27001** معيار لإدارة أمن المعلومات (الجانب الإداري والحوكمة)
- **NIST CSF** الإطار الأمريكي الأكثر مرونة وفاعلية في إدارة المخاطر (الجانب التنفيذي)
- **SOC 2** المعيار الخاص بشركات الخدمات الرقمية لضمان الخصوصية والأمان.
- **Cyber Essentials** النموذج المبسط والموجه لحماية الشركات الصغيرة والمتوسطة.

2.3.4- المقارنة التحليلية بين الأطر والمعايير الدولية للأمن السيبراني

تختلف الأطر والمعايير الدولية في أهدافها ومنهجياتها، مما يتطلب إجراء تحليل متقاطع ومقارنه بمعرفة كيفية عمل كل معيار ومنطقة التركيز الخاص به ويمكن تلخيص هذه المقارنة بالجدول التالي :

جدول رقم 3 . مقارنة بين المعايير والاطر الدوليه

البند	ISO 27001	NIST CSF	SOC 2	Cyber Essentials
نوع المعيار	معيار دولي لإدارة أمن المعلومات	إطار (Framework) لإدارة المخاطر	تقرير تدقيق (Audit Report)	برنامج شهادة أساسي للأمن السيبراني
الجهة المصدرة	المنظمة الدولية للتوحيد (ISO)	معهد المعايير والتقنية الأمريكي (NIST)	American Institute of CPAs (AICPA)	حكومة المملكة المتحدة
التركيز الرئيسي	نظام إدارة أمن المعلومات (ISMS)	إدارة المخاطر السيبرانية	ضوابط أمن الخدمات Services Trust) (Criteria	الأمن الأساسي ضد الهجمات الشائعة
النطاق	شامل وواسع (كل الشركة)	مرن وقابل للتخصيص	خاص بالخدمات السحابية والموردين	أساسي وبسيط (مناسب للشركات الصغيرة)
عدد الضوابط / المتطلبات	93 ضابط (Annex A)	5 وظائف رئيسية Protect, ,Identify)	5 معايير Trust Services	5 ضوابط أساسية فقط

		Detect, Respond, (Recover		
الجمهور المستهدف	جميع الشركات (خاصة الكبيرة والمتوسطة)	الشركات الأمريكية والحكومية بشكل أساسي	الشركات التي تتعامل مع بيانات العملاء (خاصة السحابية)	الشركات الصغيرة والمتوسطة في بريطانيا وأوروبا
مستوى الصعوبة	عالي	متوسط إلى مرتفع	عالي	منخفض (الأسهل)
التكلفة	مرتفعة	مجاني (لكن التنفيذ مكلف)	مرتفعة جداً	منخفضة نسبياً
التركيز على	الإدارة والعمليات والمخاطر	إدارة المخاطر بشكل دوري	خصوصية البيانات وأمان الخدمات	الحماية الأساسية (Firewall, Password, etc.)
التوافق مع الآخرين	عالي	مرتفع	متوسط	منخفض

المبحث الثاني: تحليل المخاطر في بيئة الشركات الصغيرة والمتوسطة(SMEs)

3.1- تحليل دوافع استهداف الشركات الصغيرة والمتوسطة

لا يعد استهداف الشركات الصغيرة والمتوسطة عشوائيًا، بل هو نتاج استراتيجية متعمدة من قبل المهاجمين تستغل «نقاط الضعف الهيكلية» في هذه الشركات .(Rombaldo Junior et al., 2023) ويمكن تحليل هذه الدوافع من خلال المحاور التالية، مع الربط بمكونات مخاطر الأمن السيبراني وفق تعريف NIST (SP 800-30 Rev. 1, 2012)والتي تهدد الركائز الثلاثة: السرية، والسلامة، والتوافر.

3.1.1- فجوة الاستثمار الأمني (دوافع مالية وهيكلية)

- محدودية الميزانية وتراكم "الدين التقني :(Security Technical Debt) "تعاني الشركات الصغيرة والمتوسطة بالقاهرة من معضلة "تخصيص الموارد"؛ حيث تُعطى الأولوية للنمو والتشغيل على حساب الأمن. هذا يؤدي إلى استخدام برمجيات غير مرخصة أو أنظمة قديمة (Legacy Systems) تجاوزت عمرها الافتراضي.

3.1.2- أزمة الكوادر البشرية و"سلبية الوعي "(دوافع تنظيمية)

- **نقص الكوادر المتخصصة :(The Talent Gap)** تفتقر معظم هذه الشركات لوجود "مسؤول أمن معلومات (CISO) " متفرغ، وغالباً ما تُسند مهام الأمن لموظف تكنولوجيا المعلومات العام .(IT Generalist) هذا يؤدي إلى غياب الرؤية الاستباقية والاكتفاء بـ "رد الفعل "عند وقوع الاختراق.

3.1.3- نظرية "حصان طروادة "(دوافع استراتيجية)

- **الشركات الصغيرة كبوابة عبور :(Supply Chain Pivoting)** يعد هذا من أخطر الدوافع؛ فالمهاجم قد لا يستهدف بيانات الشركة الصغيرة لذاتها، بل لكونها مورداً أو مقدم خدمة (Service Provider) لشركات كبرى أو جهات سيادية.

3.2- تحليل فجوة الفاعلية بين الوعي بالمخاطر واتخاذ الإجراءات الوقائيه بالشركات الصغيره والمتوسطه

من خلال تحليل واقع الأمن السيبراني في الشركات التكنولوجية، يتبين أن المشكلة الأساسية لا تكمن دائماً في "الجهل" بالمخاطر، بل في وجود فجوة واضحة بين إدراك الخطر وبين اتخاذ إجراءات وقائية فعالة لمواجهته. ويمكن تأصيل هذه الفجوة فيما يلي:

3.2.1- وهم الأمان المكتسب(Security Illusion)

تشير التقارير الدولية 2023) Verizon إلى أن الكثير من المسؤولين في الشركات الصغيرة والمتوسطة يتبنون سياسات دفاعية "ساكنة" نتيجة لعدم تعرضهم لهجمات مباشرة سابقة، أو لكون الهجمات التي تعرضوا لها كانت محدودة الأثر. هذا يؤدي إلى حالة من "الاطمئنان الزائف" الذي يجعل الاستثمار في الأمن السيبراني يبدو كأنه عبء مالي غير ضروري وليس ضرورة استراتيجية.

3.2.2- مؤشرات الفجوة في السوق المصري والعالمي

تدعم الإحصائيات الواردة في تقارير مثل (2023) Ciscoو (2023) Verizonهذا الافتراض، حيث سجلت الأسواق العالمية والمحلية (بما فيها السوق المصري) زيادة في وتيرة الإصابات السيبرانية الناجحة، رغم إعلان الشركات عن امتلاكها لبرامج توعية. هذا يدل على أن الوعي الموجود هو "وعي نظري" لا ينعكس على الإجراءات الوقائية الفعلية(Preventive Measures) ، وهو ما يؤكد حاجة هذه الشركات إلى نظام "متابعة وتقييم" لقياس فاعلية تلك الإجراءات وليس مجرد وجودها.

3.2.3- مبررات اتساع الفجوة لدى صناع القرار

يمكن حصر أسباب عدم تحويل الوعي إلى فاعلية لدي صناع القرار في النقاط التالية:

- غياب التجربة المباشرة وعدم التعرض لهجمات عنيفة يجعل من الخطر السيبراني "تهديداً نظرياً" في نظر الإدارة.
- تحجيم الأثر والاعتقاد بأن الهجمات تؤثر فقط على الشركات الكبرى أو المؤسسات المالية، وهو ما تفنده تقارير (2023) ENISAالتي تؤكد استهداف الشركات الصغيرة كحلقة أضعف.

3.3- رصد وتحليل المشهد السيبراني في السياق المصري – بالشركات الصغيره والمتوسطه

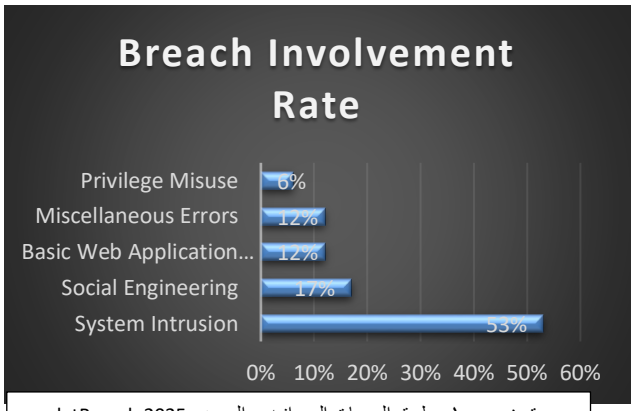
يتسم المشهد السيبراني في مصر فيما يخص الشركات الصغيره والمتوسطه بتحول رقمي متسارع تقابله تحديات أمنية متزايدة مما يجعل تقييم فاعلية الإجراءات الوقائية ضرورة حتمية وليس مجرد خيار تقني. حيث شهدت مصر خلال السنوات الخمس الماضية (2021–2026) نموًا رقميًا ملحوظًا مدعومًا بمبادرات "مصر الرقمية" ورؤية مصر 2030، مما جعلها هدفًا جذابًا للهجمات السيبرانية رغم تقدمها في مؤشرات الأمن السيبراني العالمية. حيث حققت مصر تقدمًا ملحوظًا في مؤشر الأمن السيبراني العالمي (GCI) الصادر عن الاتحاد الدولي للاتصالات (ITU) لعام 2024، حيث سجلت **100 نقطة كاملة**، مما وضعها ضمن (Role–Modelling) Tier 1 ومن بين أفضل 12 دولة عالميًا. ويُعد هذا التصنيف الأول إقليميًا في الدول العربية، مقارنة بـ95.48 نقطة في عام 2020.

وبالرغم من هذا التطور التنظيمي علي مستوي الدوله فقد أشارت تقارير INTERPOL في عام 2025 إلى أن مصر تقع ضمن **الـ20 دولة الأكثر عرضة للهجمات السيبرانية عالميًا**، مدعومًا بارتفاع معدلات الاختراق الناتج عن التحول الرقمي السريع وزيادة مستخدمي الإنترنت. ووفقًا لتقرير INTERPOL Africa Cyberthreat Assessment Report 2025 ، شكلت مصر **13%**من إجمالي الهجمات السيبرانية في أفريقيا خلال عام 2024، محتلة المرتبة الثانية بعد جنوب أفريقيا.

ويُقدر التقرير أن الخسائر السنوية الناتجة عن الجرائم السيبرانية في مصر تتجاوز مليارات الدولارات، مع تصاعد التهديدات المرتبطة بالدفع الإلكتروني والخدمات الرقمية.

3.3.1- أنواع ومعدلات الهجمات السيبرانية الرئيسية(2021-2026)

أظهر تقرير Positive Technologies حول الهجمات على البنية التحتية المصرية في عام 2024 أن أبرز طرق الهجوم كانت **الهندسة الاجتماعية (Social Engineering)** و**تنفيذ الرموز عن بعد(Remote Code Execution)** ، بنسبة **36%** لكل منهما (72% مجتمعين). وشملت الهجمات البارزة DDoS على شركتي Vodafone و Etisalat(توقف الخدمات لأكثر من 5 ساعات)، وهجوم Ransomwareعلى مصلحة الضرائب (تشفير وسرقة 500 جيجابايت من البيانات)، بالإضافة إلى اختراقات أدت إلى تسريب بيانات ملايين المواطنين وبيعها على الدارك ويب.

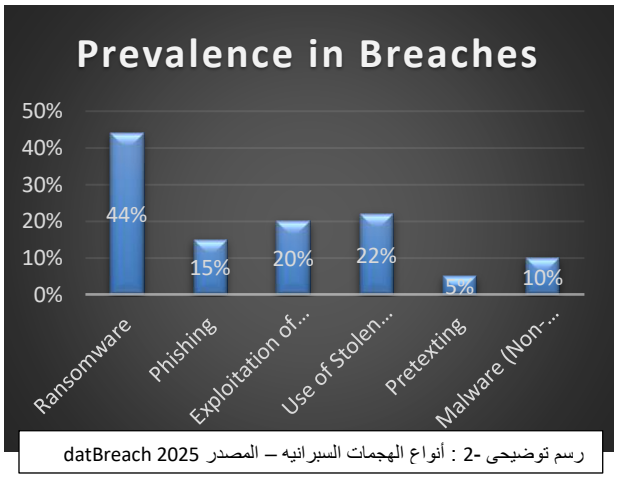


رسم توضيحي -١ : طرق الهجمات السبرانيه – المصدر datBreach 2025

كما سجل التقرير انتشار الـ Ransomware كأحد أبرز التهديدات في شمال أفريقيا، حيث تعرضت مصر لـ12,281 كشفًا عن هجمات Ransomware في 2024 (مقارنة بـ17,849 في جنوب أفريقيا). أما تقرير IBM Cost of a Data Breach Report 2025، فقد أشار إلى انخفاض متوسط تكلفة الاختراق في الشرق الأوسط (بما في ذلك نموذج مصر) بنسبة 18% ليصل إلى حوالي **27مليون ريال سعودي**)نحو 7.2 مليون دولار أمريكي.(

3.3.2- الهجمات الموجهة إلى الشركات الصغيرة والمتوسطة(SMEs)

تُعد الشركات الصغيرة والمتوسطة الأكثر عرضة للهجمات بسبب محدودية الموارد المالية والفنية، وضعف الاستثمار في الأمن السيبراني، وعدم كفاية التدريب على الوعي الأمني أثناء التحول الرقمي. فقد أكد تقرير Verizon Data Breach Investigations Report (DBIR) 2025 أن الـ Ransomware يشكل **88%** من الاختراقات في الشركات الصغيرة والمتوسطة، مقارنة بـ**39%** فقط في الشركات الكبرى. وفي السياق المصري، تستهدف الهجمات قطاعات التصنيع والتجارة الإلكترونية والنقل والخدمات، حيث



رسم توضيحي -2 : أنواع الهجمات السبرانيه – المصدر datBreach 2025

أدت بعض الحوادث إلى تسريب بيانات ملايين العملاء **كمثال واقعة اختراق بيئة اختبار شركة فوري (القاهرة 24، 2023).**

3.4- رصد وتحليل البيئه التشريعيه وتوجهت الدوله المصريه

3.4.1- البيئة التشريعية والمخاطر القانونية (قانون رقم 151 لسنة 2020)

يمثل قانون حماية البيانات الشخصية رقم 151 لسنة 2020 حجر الزاوية في المنظومة التشريعية السيبرانية المصرية. وتتمثل أبرز محاوره في الجوانب التالية:

- **حقوق الشخص المعني بالبيانات** :منح الأفراد حق الوصول إلى بياناتهم، وتصحيحها، أو الاعتراض على معالجتها، مع وجوب الحصول على موافقتهم الصريحة قبل جمع البيانات.
- **التزامات المتحكم والمعالج** :فرض التزامات تقنية وإدارية على الشركات (المتحكم/المعالج) لضمان سرية وسلامة البيانات، مع ضرورة تعيين «مسؤول حماية بيانات.(DPO) «
- **إنشاء مركز حماية البيانات الشخصية** :وهو الجهة التنظيمية المسؤولة عن منح التراخيص، والمراقبة، وتلقي البلاغات عن أي اختراقات.
- **تأمين البيانات العابرة للحدود** :وضع شروط صارمة لنقل البيانات خارج مصر لضمان توفر مستوى حماية مماثل.

3.4.2- إبراز الفجوة التشريعية(The Legislative Gap)

تكمن الفجوة الأساسية التي يعالجها هذا البحث في «غياب اللائحة التنفيذية» للقانون حتى تاريخه، مما أدى إلى عدد من الآثار السلبية، أبرزها:

- **ضبابية المعايير التقنية** :يطالب القانون الشركات باتخاذ «إجراءات كافية» لحماية البيانات، إلا أنه في غياب اللائحة لا تعرف الشركات – خاصة الصغيرة والمتوسطة – ما هي المواصفات الفنية المحددة التي تعتبرها الدولة «كافية.«
- **غياب المسار الإجرائي للامتثال** :لا توجد حاليًا آلية واضحة للحصول على التراخيص المطلوبة لمعالجة البيانات، مما يضع الشركات في موقف «الانتظار السلبي.«

يخلص الباحث إلى أن التحدي لا يكمن في «نص القانون» – الذي وضع بسببه منظمة الاتحاد الدولي للاتصالات (ITU)مصر في المستوى الأول (Tier 1) كما ورد في تقرير 2024 – بل يكمن في «فاعلية التطبيق». إن هذه الفجوة التشريعية تجعل من عملية «المتابعة والتقييم» داخل الشركات عملية صعبة. ففي غياب لائحة تنفيذية تمثل «المسطرة القياسية»، تضطر الشركات للاعتماد على اجتهادات فنية قد لا تصمد أمام المساءلة القانونية لاحقًا. وهذا هو المبرر الأساسي لهذا البحث: تطوير إطار عمل يساعد الشركات على تحقيق «أقصى فاعلية ممكنة» للإجراءات الوقائية بما يتماشى مع روح القانون تحسبًا لصدور لائحته.

القسم الثالث: الدراسة الميدانية ومنهجية البحث

منهجية الدراسة وإجراءاتها

يهدف هذا الفصل إلى توضيح الخطوات العلمية التي اتبعها الباحث للإجابة على تساؤلات الدراسة وتحقيق أهدافها، بدءاً من اختيار المنهج العلمي المناسب، مروراً بتحديد مجتمع الدراسة وعينتها، وصولاً إلى بناء أدوات جمع البيانات وتحليلها، وانتهاءً بآلية تقييم فاعلية الإجراءات الوقائية وتحليل الفجوة بين الواقع الميداني والمعايير الدولية والمحلية.

منهج البحث(Research Methodology)

تعتمد هذه الدراسة على المنهج الوصفي التحليلي التطبيقي وذلك لملاءمته لطبيعة البحث الذي يسعى إلى تقييم واقع الأمن السيبراني وفاعلية الإجراءات الوقائية في الشركات الصغيرة والمتوسطة، مع تقديم إطار عملي مطوَّر يتناسب مع إمكانياتها.

ويتجسد هذا المنهج في ثلاثة مستويات أساسية:

- **المنهج الوصف**

يتم من خلاله رصد وتوصيف الواقع الميداني للأمن السيبراني في الشركات محل الدراسة، وتحديد المسببات الرئيسية للتهديدات، ونوعية المخاطر التي تواجه الأصول الرقمية. ويوفر هذا المستوى قاعدة بيانات دقيقة عن الوضع الراهن.

- **المنهج التحليلي**

يقوم على معالجة البيانات إحصائياً لتحليل العلاقات بين متغيرات الدراسة (مثل العلاقة بين ضعف الوعي البشري وحجم الشلل التشغيلي)، ويشمل تحليل الفجوة بين الممارسات الحالية في الشركات المصرية والمتطلبات المعيارية الدولية.

- **المنهج التطبيقي**

يتمثل في صياغة إطار عمل مقترح ومطوَّر لحماية الأصول الرقمية وضمان استمرارية الأعمال. ولا يعتمد هذا الإطار على محاكاة جامدة لمعيار دولي واحد، بل يرتكز على منهجية الانتقاء والتطويع من خلال:

اختيار العناصر الأكثر كفاءة وملاءمة من الأطر الدولية (مثل NIST CSF 2.0 و ISO 27001) ودمجها في قالب يتناسب مع الموارد المالية والبشرية المحدودة للشركات الصغيرة والمتوسطة..

4.1 مجتمع وعينة الدراسة

مجتمع الدراسة يتكون مجتمع الدراسة من كافة شركات تكنولوجيا المعلومات والاتصالات الصغيرة والمتوسطة (Tech SMEs)التي يقع مقرها الرئيسي أو مراكز عملياتها داخل محافظة القاهرة. وقد تم اختيار هذا المجتمع للأسباب الآتية:

المركزية: تمثل القاهرة الكبرى المركز الإداري والتقني الأول في مصر، وتضم أكبر تجمع للشركات التكنولوجية الناشئة والمتوسطة (حيث تستحوذ على نسبة كبيرة من الشركات الناشئة في مصر.

عينة الدراسة: نظراً لطبيعة الدراسة التحليلية والتطبيقية، تم اختيار عينة مكونة من (**30**) شركة تكنولوجية داخل نطاق محافظة القاهرة الكبرى. وتم اختيار العينة بأسلوب **العينة القصدية** لضمان شمول شركات متخصصة في مجالات متنوعة (البرمجيات، الشبكات، الخدمات السحابية، والاتصالات–مقاولات تكنولوجية). وقد اعتمد الباحث الضوابط التالية في اختيار الشركات:

–النطاق الجغرافي: أن يكون المقر الرئيسي داخل حدود محافظة القاهرة الكبرى.

–الحجم والنشاط: تصنيف الشركة كمنشأة صغيرة أو متوسطة، مع ارتباط نشاطها الأساسي بقطاع التكنولوجيا والاتصالات.

–الجاهزية للمشاركة: اختيار الشركات التي أبدت تعاوناً في الإجابة على الاستبيان وتقديم المعلومات اللازمة.

4.2 أدوات جمع البيانات (Data Collection Tools)

اعتمد الباحث على أداتين أساسيتين لتحقيق أهداف الدراسة:

4.2.1 الاستبانة :(Questionnaire)

تمثل الأداة الرئيسية لهذه الدراسة في استبانة إلكتروني صُمم خصيصاً لجمع البيانات الأولية من الشركات التكنولوجية بمحافظة القاهرة. ويتكون الاستبيان في صورته النهائية من **31** سؤالاً، موزعة على أربعة محاور رئيسية بخلاف البيانات العامة، وهي كالتالي:

- المحور الأول: الوعي بمسببات ودوافع وخطورة التهديدات السيبرانية و يهدف هذا المحور إلى تحديد "الجذور المسببة" للمخاطر، سواء كانت تقنية أو بشرية أو ناتجة عن التعامل مع موردين خارجيين)

- المحور الثاني مدى الالتزام التشريعي وحوكمة البيانات.
- المحور الثالث: واقع الجاهزية وآليات المتابعة والتقييم :يُعد هذا المحور هو الأكبر والأكثر تفصيلاً، حيث يغطي الممارسات الحالية من (سياسات تشغيلية، أدوات حماية، إجراءات توعية، سجلات الحوادث، وخطط التعافي).
- المحور الرابع:تحديد الدوافع للامتثال للمعايير الدولية، وتحديد الأطر المفضلة وجهات الدعم الفني المستهدفة.

- **صدق استمارة الاستبانة**

تم التحقق من سلامة الأداة عبر عرضها على خبراء متخصصين في الأمن السيبراني والإحصاء لضمان دقة الصياغة ومواءمتها للأهداف البحثية.

- **ثبات استمارة الاستبانة**

للتحقق من ثبات الاستبانة وقدرته على إعطاء نتائج متسقة عند إعادة تطبيقه على عينة مماثلة، قام الباحث بإجراء اختبار الثبات باستخدام معامل ألفا كرونباخ(Cronbach's Alpha) .

وقد اعتمد الباحث في إجراء هذه التحليلات الإحصائية وحساب المعاملات على بيئة تحليل البيانات المتقدمة المدعومة بالذكاء الاصطناعي(AI-Powered Computational Environment) ، وذلك عبر استخدام لغات البرمجة الإحصائية (Python) لمعالجة بيانات العينة الاستطلاعية. وجاءت نتائج معامل الثبات لمحاور الدراسة الأربعة بناءً على الاستجابات الفعلية لعينة الدراسة (N=30) كما هو موضح في الجدول التالي:

جدول رقم :(3) معامل ألفا كرو نباخ لمحاور الاستبانة باستخدام التحليل البرمجي المحوسب

المحور	عدد الاسئله (الكمية)	قيمة معامل ألفا كرونباخ	التقييم الإحصائي
المحور الأول: إدراك التهديدات ونقاط الضعف	4	0.77	جيد جداً
المحور الثاني: الالتزام بالتشريعات الوطنية	4	0.77	جيد جداً
المحور الثالث: الجاهزية والسياسات وآليات المتابعة	6	0.73	جيد
المحور الرابع: تحديات تبني الأطر ومسارات التطوير	2	0.37	منخفض (تعدد أبعاد)
إجمالي الاستبيان	16	0.68	مقبول ومعتمد

توضح النتائج المستخلصة عبر بيئة التحليل الذكية ما يلي:

- حقق المحور الأول والمحور الثاني قيم ثبات مرتفعة بلغت(0.77) ، مما يشير إلى اتساق عالٍ جداً في إجابات المبحوثين فيما يتعلق بإدراك المخاطر السيبرانية والوعي بالتشريعات الوطنية، وهو ما يعزز الثقة في صدق استجابات العينة لهذين المحورين.
- سجل المحور الثالث (الجاهزية والـ(M&E ، وهو المحور الجوهري للدراسة، قيمة(0.73) ، وهي قيمة تتجاوز الحد الأدنى المقبول إحصائياً (0.60)، مما يؤكد أن فقرات المحور تقيس بصدق وثبات مستويات النضج والجاهزية التشغيلية للشركات محل الدراسة.
- بالنسبة لـ المحور الرابع، فقد سجل قيمة(0.37) ، ويُعزى ذلك إحصائياً إلى طبيعة المحور التي تقيس "عوائق وتحديات متنوعة" (بشرية ومالية) قد لا ترتبط ببعضها بالضرورة في الواقع العملي، بالإضافة إلى محدودية عدد الفقرات الداخلة في الاختبار الإحصائي لهذا المحور.
- بلغ معامل الثبات الكلي للاستبيان (0.68)، وهي قيمة مقبولة ومعتمدة في الدراسات التطبيقية المماثلة، مما يؤكد أن أداة الدراسة تتمتع بدرجة كافية من الاستقرار والاتساق الداخلي، وصالحة تماماً لتحليل النتائج في الفصول اللاحقة.

4.3- منهجية دراسة الحالة

اعتمد الباحث على منهج "دراسة الحالة" كمنهج نوعي مكمل للمنهج الكمي المتمثل في الاستبيان، وذلك بغرض التعمق في فهم الآليات الفعلية لإدارة المخاطر السيبرانية داخل الشركات المتوسطة بقطاع التكنولوجيا بالقاهرة.

4.3.1- مبررات اختيار حالة الدراسة (شركة X وتم حجب اسم الشركه بناءا علي رغبتها)

وقع اختيار الباحث على شركة **X** للاتصالات لتكون نموذجاً تطبيقياً للدراسة بناءً على المعايير التالية:

- التمثيل القطاعي: تعمل الشركة في قطاع تكنولوجيا المعلومات والاتصالات.
- الحجم التنظيمي: تندرج الشركة ضمن فئة "الشركات المتوسطة" (100 موظف)، وهي الفئة التي تمتلك بنية تحتية تقنية متطورة ولكنها تواجه تحديات في الموارد المخصصة للأمن السيبراني.
- التعرض الفعلي للمخاطر: سجلت الشركة حوادث اختراق ناجحة ومتنوعة (خارجية، تقنية، وداخلية)، مما يوفر مادة خصبة لتحليل فعالية إجراءات الاستجابة والتعافي.
- البنية الهجينة: تعتمد الشركة على مزيج من الخوادم الداخلية والخدمات السحابية.

4.3.2- أدوات جمع بيانات دراسة الحالة

استخدم الباحث أداة "المقابلة شبه الموجهة" (Semi-structured Interview) مع الكوادر الفنية المسؤولة عن أمن البيانات بالشركة، وقد تمحورت الأسئلة حول النقاط التالية:

1. توصيف الهيكل التنظيمي والتقني المسؤول عن حماية البيانات.
2. سرد وتحليل وقائع حوادث الاختراق التي تعرضت لها الشركة (التوقيت، الأسلوب، الخسائر).
3. تقييم كفاءة الأنظمة الدفاعية (Firewalls) مقابل الأخطاء البشرية والإدارية.
4. رصد آليات المتابعة والتقييم (E&M) المتبعة بعد وقوع الحوادث ومدى تطور الوعي الأمني للإدارة.

القسم الرابع: تحليل نتائج الدراسة الميدانية واختبار التساؤلات

5.1- الخصائص العامة لعينة الدراسة توصيف الشركات

وفقا لأهداف البحث تم استخدام أسلوب العينة القصدية والتي تتميز بالعمل في مجال التكنولوجيا الرقمية والاتصالات سواء مجال الخدمات او المشاريع الرقمية وتقع في نطاق محافظة القاهرة – وكان حجم العينة (30) شركه وكانت سماتها كالتالي.

5.1.1: توزيع الشركات حسب حجم عدد الموظفين:

جدول رقم 5 : توزيع الشركات حسب الحجم بعينة الدارسه

فئة حجم الشركة (عدد الموظفين)	التكرار (عدد الشركات)	النسبة المئوية
من 1 إلى 5 موظفين	3	٪10
من 5 إلى 20 موظف	11	٪37
من 20 إلى 100 موظف	7	٪23
من 100 إلى 250 موظف	9	٪30
الإجمالي	30	%100.00

ركز الباحث علي ضرورة ان تشمل العينة تنوع في حجم الشركات من ناحية عدد الافراد والذي سوف ينعكس علي الإجراءات المتبعة في تأمين البيئة الرقمية بالشركة.

5.2- التحليل الاحصائي لمحاور البحث

جدول رقم 6 : الحصر الكمي لنتائج الاستبيا

المحور	رقم السؤال	مضمون السؤال	1	2	3	4	5	المتوسط	الانحراف المعياري
المحور الأول: إدراك التهديدات السيبرانية ونقاط الضعف	س4	هل تعتقد ان جميع الشركات معرضة لتهديدات سيبرانية بغرض التخريب او السرقة او الابتزاز او ايقاف الاعمال او التجسس؟	0	1	4	5	20	4.8	0.92
	س5	هل تعتقد انه يمكن التجسس عليك او سرقة بيانات هامه لدي الشركه او غير ذلك من الاثار السلبيه للهجمات السيبرانيه – دون ان تكتشف ذلك؟	0	3	2	8	17	4.6	1.04
	س7	هل تعتقد أن الاعتماد المتزايد على التكنولوجيا في العمليات اليومية مع ضعف الوعي الامني لدى الكوادر البشرية يمثل التهديد الرئيسي لاحتمالية التاثر سلبيا بهجمات سيبرانيه؟	3	0	0	9	18	4.6	1.25
	س16	هل الإفصاح (الإعلان) عن التعرض لهجمات سيبرانيه ناجحه قد يؤثر علي سمعة الشركه او بيئة اعمال الشركه – وبالتالي يتم التعامل مع الهجمات بسريه تامه واخفاء تاثيرها؟	3	2	9	5	11	3.9	1.35
		الاجمالي						**4.47**	**1.14**
المحور الثاني: الالتزام بالتشريعات الوطنية (قانون 2020/151)	س9	ما مدي إلمامك (معرفتك) بالمبادرات الوطنيه والقوانين والتشريعات المصريه لتنظيم الامن السيبراني؟	5	4	14	4	3	3.1	1.19
	س10	ما مدي التزام شركتك بالقوانين والتشريعات المصرية المنظمه لحماية البيانات الشخصية وإجراءات الامن السيبراني؟	2	2	8	8	10	4.0	1.23
	س14	تواجه الشركه حاليا صعوبات تنظيمية أو مالية تحول دون الالتزام الكامل بالتشريعات الوطنية للأمن السيبراني؟	7	3	14	4	2	2.9	1.20

	س15	هل توافق علي ان الالتزام بالتشريعات الوطنية، خاصة قانون 2020/151، سوف يساعد في تقليل مخاطر الانتهاكات السيبرانية في الشركات الصغيرة والمتوسطة؟	1	2	7	15	5	4.0	0.99
		الاجمالي						**3.5**	**1.15**
المحور الثالث: الجاهزية والسياسات وآليات المتابعة (E&M)	س6	هل تتفق مع التقارير التي تفيد ان الشركات المصرية (الصغيره والمتوسطه) مستعده – بدرجه كبيره– لمواجهة أي تهديدات سيبرانية معقده؟	7	8	8	2	3	2.5	1.26
	س12	هل يتم تطبيق سياسات وتعليمات صارمه بالشركه لتعزيز الامن السيبراني؟	5	3	3	10	9	3.8	1.48
	س20	هل توافق عل ان احد السياسيات التي يجب تطبيقها بالشركه هو الاعتماد علي البرامج الاصليه فقط في اعمال الشركه؟ (تم نقله هنا لتعزيز الثبات)	1	0	8	6	15	4.4	1.08
	س21	هل يوجد ميزانيه مخصصه سنويا لتحديث برامج الفيروسات وتراخيص انظمة الجدار الناري وشراء الاصدارات الحديثه من التطبيقات والبرامج؟	0	8	5	12	5	3.7	1.10
	س24	تقييم/مراجعة الأمن السيبراني داخل الشركة دورياً – شيء ضروري للشركه؟	0	1	5	7	17	4.6	0.94
	س26	لدي توجد خطة معتمدة لاستعادة البيانات (Disaster Recovery) في حال وقوع اختراق او تلف لها؟	4	0	3	21	2	3.8	1.13
		الاجمالي						**3.8**	**1.14**
المحور الرابع: تحديات تبني الأطر الدولية ومسارات التطوير	س22	هل تري ان التدريب الدوري لزيادة الوعي داخل الشركه هام جدا لمواجهة الهجمات السيبرانيه؟	0	1	6	3	20	4.7	0.99
	س30	تواجه الشركات تحديات في تبني واتباع الأطر الدولية (Framework) للأمن السيبراني بسبب نقص الموارد و الكفاءات البشرية؟	1	2	12	8	7	3.9	1.07
	س31	تواجه الشركات تحديات في تبني الأطر (Framework) الدولية للأمن	1	4	10	6	9	3.9	1.19

		السيبراني بسبب نقص الموارد – المالية –؟							
		الاجمال						4.17	1.08

5.2.1- تحليل النتائج الإحصائية لتقييم فاعلية الإجراءات الوقائية للأمن السيبراني في الشركات الصغيرة والمتوسطة

أظهرت نتائج الدراسة الميدانية مستوى عاليًا من الإدراك النظري للتهديدات السيبرانية ضمن المحور الأول، حيث سجل السؤال الرابع متوسطًا مرتفعًا جدًا (4.8) بانحراف معياري منخفض (0.92)، مما يعكس إجماعًا قويًا بين المستجيبين على تعرض جميع الشركات لمختلف أشكال التهديدات (تخريب، سرقة، ابتزاز، تجسس). كما أكدت الأسئلة 5 و7 (متوسط 4.6 لكليهما) وجود وعي واضح بإمكانية وقوع هجمات غير مكتشفة وبأن الاعتماد المتزايد على التكنولوجيا مع ضعف الوعي البشري يمثل التهديد الرئيسي.

وعليه فان نتائج المحور الأول بينت وجود وعي نظري مرتفع جداً بالمخاطر السيبرانية (بمتوسط (4.475، يقابله تباين ملحوظ وحذر تجاه الإفصاح عن الاختراقات؛ مما يؤكد فجوة "الوعي السلبي "والحاجة لإطار عمل يوازن بين الحماية الصارمة والخصوصية المؤسسية.

أما المحور الثاني المتعلق بالالتزام بالتشريعات الوطنية (قانون 2020/151) فقد كشف عن فجوة واضحة؛ إذ بلغ متوسط الإلمام بالمبادرات والقوانين المصرية (3.1) فقط، بينما جاء التزام الشركات بالتشريعات أعلى نسبيًا (متوسط 4.0). ومع ذلك، لم يرَ المستجيبون صعوبات تنظيمية أو مالية كبيرة تحول دون الالتزام (متوسط 2.9)، وأبدوا اتفاقًا قويًا على أن الالتزام بالقانون سيقلل من المخاطر (متوسط 4.0) .

وعليه فقد اظهرت بيانات المحور الثاني وجود فجوة جوهرية بين الإدراك النظري المرتفع للمخاطر والتشريعات وبين واقع الممارسة التقنية المحدودة نتيجة 'الوعي السلبي 'ونقص الموارد والمخاوف المتعلقة بالسمعة.

وفي المحور الثالث الخاص بالجاهزية والسياسات وآليات المتابعة، برز تناقض واضح بين الوعي النظري والواقع العملي: فقد سجل السؤال السادس أدنى متوسط في الدراسة (2.5) مما يعني رفضًا واضحًا لفكرة أن الشركات المصرية الصغيرة والمتوسطة مستعدة بدرجة كبيرة لمواجهة التهديدات المعقدة. وعلى الرغم من اتفاق المستجيبين على ضرورة المراجعة الدورية للأمن السيبراني (4.6) والاعتماد على البرامج الأصلية (4.4)، إلا أن تطبيق السياسات الصارمة (3.8)، تخصيص ميزانية سنوية للتحديثات (3.7)، ووجود خطة معتمدة لاستعادة البيانات (Disaster Recovery) (3.8) جاءت جميعها في النطاق المتوسط، مما يشير إلى ضعف التنفيذ العملي للإجراءات الوقائية .

وهكذا كشفت نتائج المحور عن قناعة مؤسسية مرتفعة بأهمية التدقيق الدوري والبرمجيات الأصلية (3.8) متوسط إلا أنها أظهرت فجوة حادة في الجاهزية الفعلية لمواجهة التهديدات المعقدة؛ مما يعزز فرضية الدراسة بأن التحدي لا يكمن في الإدراك، بل في القدرة على التنفيذ والامتثال الإجرائي

أما المحور الرابع المتعلق بتحديات تبني الأطر الدولية فقد اظهر التحدي الأكبر يتمثل في **نقص الموارد البشرية والمالية** (متوسط 3.9)، مما يعيق تبني وتطبيق الأطر الدولية مثل.(NIST, ISO 27001, CIS Controls) – وعليه فبالرغم من الوعي المرتفع بأهمية بناء القدرات البشرية، إلا أن الشركات لا تزال تواجه صعوبة حقيقية في تخصيص الموارد اللازمة لتبني الأطر الدولية بشكل كامل

5.2.2- ملخص تحليل نتائج أسئلة الاستبانة بنظام ليكارت

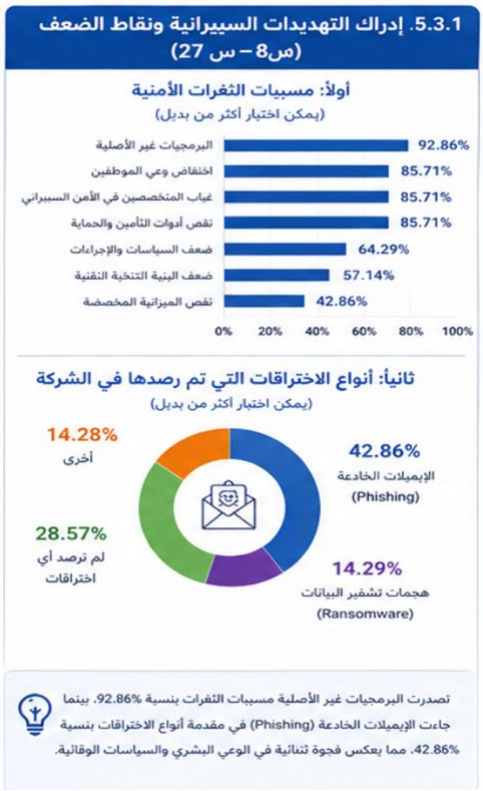
تؤكد نتائج الدراسة وجود وعي نظري مرتفع بالتهديدات السيبرانية، إلا أن التباين (الانحراف المعياري) الكبير في الأسئلة التنفيذية يكشف عن تشتت واضح في مستويات الاستعداد بين الشركات، مما يعكس فجوة جوهرية بين الإدراك النظري العالي والالتزام الضعيف نسبيًا بالإجراءات الوقائية الفعلية. وبالتالي، فإن فعالية الإجراءات الوقائية للأمن السيبراني في الشركات الصغيرة والمتوسطة لا تزال محدودة، وهذا يبرر الحاجة الملحة إلى حلول مخصصة حسب حجم الشركة وقطاعها، مع تدخلات مؤسسية وتشريعية أقوى لسد هذه الفجوة.

5.3- تحليل أسئلة الاختيار المتعدد في تقييم فاعلية الإجراءات الوقائية للأمن السيبراني

5.3.1- إدراك التهديدات السيبرانية ونقاط الضعف (س8 – س 27)

كشفت نتائج أسئلة الاختيار المتعدد عن فجوة أمنية حرجة تؤكد ما سبق رصده في تحليل مقياس ليكارت. حيث تصدرت – البرمجيات غير الأصلية– مسببات الثغرات بنسبة **92.86٪**، تلتها بالتساوي "انخفاض وعي الموظفين"، "غياب المتخصصين"، و نقص أدوات التأمين بنسبة **85.71٪** لكل منها.أما أنواع الاختراقات الفعلية، فقد جاءت "الإيميلات الخادعة "(Phishing) في المقدمة بنسبة **42.86٪**، تلتها "هجمات تشفير البيانات "(Ransomware)بنسبة **14.29٪** .ورغم أن **28.57٪** من العينة لم ترصد أي اختراقات، إلا أن النسب المرتفعة لمسببات الثغرات تشير إلى احتمال وجود هجمات كامنة غير مكتشفة.

تدعم هذه النتائج المتوسطات المنخفضة في محور الجاهزية، وتؤكد الحاجة الملحة إلى تعزيز الوعي البشري وتفعيل سياسات حوكمة أمنية فعالة في الشركات الصغيرة والمتوسطة.

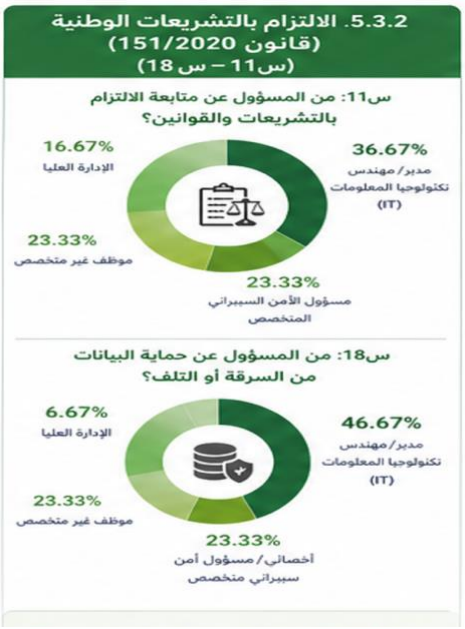


رسم توضيحي رقم ٣ : تحليل محور الوعي – المصدر google gemini generation tool

5.3.2- الالتزام بالتشريعات الوطنية (قانون 2020/151)

أظهرت نتائج أسئلة الاختيار (س11 – س18) المتعدد تمركزًا واضحًا للمسؤولية الأمنية والقانونية على مدير أو مهندس تكنولوجيا المعلومات(IT) ، حيث بلغت نسبته **36.67٪** في متابعة الالتزام بالقوانين (س11)، وارتفعت إلى **46.67٪** في حماية البيانات من السرقة أو التلف (س18). كما تساوت نسبة الاعتماد على "مسؤول الأمن السيبراني المتخصص "مع "الموظف غير المتخصص "عند **23.33٪** لكل منهما في السؤالين. وتعكس هذه الأرقام فجوة تخصصية في حوكمة الشركات الصغيرة والمتوسطة، حيث يُلقى العبء الأساسي على قسم الـ ITالتقليدي، مع غياب التمييز الواضح بين المسؤوليات التشغيلية والرقابة الأمنية.

ويؤدي هذا التداخل إلى إضعاف آليات المتابعة والتقييم، ويجعل الإجراءات الوقائية تعتمد على الاجتهادات الفردية أكثر من السياسات المؤسسية المتخصصة.



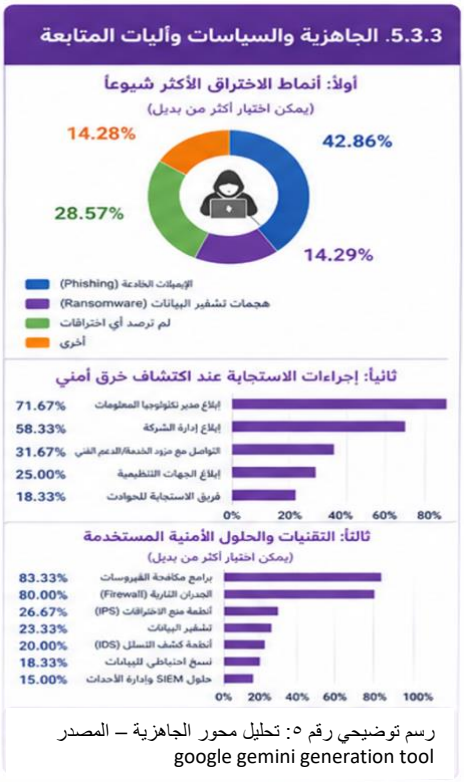
رسم توضيحي رقم ٤ : تحليل محور الالتزام التشريعي – المصدر google gemini generation tool

5.3.3- اسئلة الجاهزية والسياسات وآليات المتابعة

تكشف النتائج عن واقع مقلق في مواجهة التهديدات السيبرانية داخل الشركات التكنولوجية محل الدراسة. حيث تتصدر **الإيميلات الخادعة (Phishing)** أنماط الاختراق بنسبة **42.86٪**، متفوقًا بفارق كبير على **هجمات تشفير البيانات (Ransomware)** التي بلغت **14.29٪** .ويعكس هذا الانتشار الواسع للهجمات الاجتماعية الهندسية ضعف الوعي البشري والتدريب، مؤكدًا أن العنصر البشري لا يزال الحلقة الأضعف في سلسلة الدفاع.

أما إجراءات الاستجابة عند اكتشاف الخرق، فتنحصر في المسارات التقليدية مثل إبلاغ **مدير تكنولوجيا المعلومات (IT Manager)** أو إدارة الشركة مباشرة. ويشير هذا الاعتماد على الإبلاغ الهرمي إلى غياب آليات استجابة مؤسسية منظمة وسريعة، مما يزيد من احتمال تأخير الاحتواء وتفاقم الأضرار.

اما تقنيًا، فتعتمد الغالبية العظمى على حلول دفاعية تقليدية، حيث بلغ استخدام برامج مكافحة الفيروسات 83.33٪ والجدران النارية **80٪**، مقابل تراجع حاد في الحلول الاستباقية مثل أنظمة منع الاختراقات (IPS) بنسبة **26.67٪** وتشفير البيانات بنسبة 23.33٪ فقط.



رسم توضيحي رقم ٥: تحليل محور الجاهزية – المصدر google gemini generation tool

وعليه فان هذه المؤشرات مجتمعة تؤكد أن الشركات المبحوثة تتبنى استراتيجية "رد الفعل "الدفاعية حيث تعتمد على الدفاعات السطحية والاستجابة بعد الحادث، وتفتقر إلى الحماية في العمق والكشف المبكر والتحليل الاستباقي. وبالتالي، تبقى الأصول الرقمية عرضة لمخاطر عالية عند تجاوز الطبقات الأولية.

5.3.4- تحديات تبني الأطر الدولية ومسارات التطوير

وفيما يخص الأطر الدولية المستخدمة لتأمين الشركات ضد الهجمات السيبرانية، أظهرت النتائج فجوة معرفية كبيرة، حيث أفاد نصف العينة (50٪) بأنهم لم يسمعوا بهذه الأطر ولا يستخدمونها. ويمثل هذا الواقع تحديًا جوهريًا في قطاع الشركات التكنولوجية بالقاهرة، إذ يعني غياب اللغة الموحدة والمنهجية العلمية في إدارة المخاطر لدى نصف الشركات المستطلعة. ومع ذلك، يتصدر إطار ISO 27001قائمة الأطر المعروفة بنسبة 21٪، مما يعكس ميل الشركات التكنولوجية في مصر نحو الأطر التي توفر شهادات اعتماد معترف بها عالميًا، سواء لأغراض تسويقية أو قانونية.

الأمن السيبراني.

«صدمة» قانونية أو تشغيلية حقيقية قبل أن تستثمر استثمارًا جادًا في

من خطورة الابتزاز والخسارة المالية، إلا أنهما لم يتصدرا قائمة الدوافع الاستباقية، مما يعزز فكرة أن العديد من الشركات قد تحتاج إلى

بضرورة تطوير البيئة الرقمية داخل الشركة لمواجهة التهديدات. وبالرغم

عائق إداري من أعلى إلى أسفل يتمثل في نقص الوعي لدى الإدارة العليا

وليس اختيارية لرفع مستوى الالتزام بالأمن السيبراني. كما يبرز وجود

بنسبة تقارب 29٪. ويؤكد هذا الرقم أهمية الإطار التشريعي كأداة إجبارية

بتحليل الدوافع التي تدفع الشركات للامتثال وتطبيق إجراءات وقائية صارمة فقد لوحظ ان الضغط القانوني والتنظيمي في جاء بالمرتبة الأولى

5.4- دراسة العلاقات ومعامل الارتباط بين متغيرات الدراسة

رسم توضيحي رقم ٦: تحليل معامل الارتباط – المصدر google gemini generation tool

5.4.1- العلاقة بين توفر الميزانية وتطبيق أدوات الحماية السيبرانية

أظهرت نتائج تحليل الارتباط وجود **علاقة إيجابية قوية ودالة إحصائياً** بين متغير "توفر الميزانية المخصصة للأمن السيبراني" (س21) ومتغير "تطبيق الأدوات والحلول التكنولوجية لتعزيز الأمن السيبراني" (س 19) حيث بلغ معامل ارتباط بيرسون (r=0.831, P<0.01) ومعامل سبيرمان (rho=0.809, P<0.01). يشير هذا الارتباط القوي إلى أن **توفر**

الموارد المالية يُعدّ من العوامل الحاسمة في رفع مستوى الجاهزية التقنية للشركات، مما يؤكد فرضية البحث المتعلقة بنقاط الضعف المالية والتقنية.

5.4.2- العلاقة بين حجم الشركة ومستوى النضج السيبراني العام

كشف تحليل الارتباط عن **علاقة إيجابية قوية ودالة إحصائياً** بين حجم الشركة (عدد الموظفين) ومستوى النضج السيبراني العام، حيث بلغ معامل بيرسون **($r = 0.766, p<0.01$)** ومعامل سبيرمان **($rho = 0.740, p<0.01$)** اوضح التحليل الوصفي أن مستوى النضج يرتفع بشكل ملحوظ مع زيادة حجم الشركة، حيث سجلت الشركات التي تضم من **100إلى 250 موظفاً** متوسط درجة نضج قدره **81.4%** مستوى مدار ومستدام، بينما سجلت الشركات الصغيرة جداً (أقل من 5 موظفين) متوسطاً منخفضاً قدره **37.7%** مستوى متدني. ويؤكد هذا أن حجم الشركة يُعد متغيراً حاسماً في قدرتها على تخصيص الموارد المالية والبشرية والتقنية اللازمة لتعزيز الأمن السيبراني.

5.4.3- العلاقة بين إدراك المخاطر والالتزام بالتشريعات الوطنية

كشف تحليل الارتباط عن **علاقة عكسية قوية** بين محور "إدراك المخاطر والنقاط الضعيفة السيبرانية" (المحور الأول) ومحور "الالتزام بالقانون رقم 151 لسنة 2020" (المحور الثاني). يشير هذا الارتباط العكسي إلى أن الشركات التي تدرك مخاطرها السيبرانية بشكل أكبر غالبًا ما تكون **أقل التزاماً** بالتشريعات الوطنية. وقد يعكس ذلك وجود **فجوة واضحة** بين الوعي النظري بالمخاطر والقدرة على التنفيذ العملي، أو نقص القدرات التنفيذية رغم ارتفاع مستوى الوعي.

5.5- تقييم العينة وفقا للمحاور البحث الأربعة

الغرض من التقييم هو رصد مدي الجاهزية لدي الشركات التكنولوجية الصغيرة والمتوسطة ومقارنتها بالنسب العالمية لذلك سيتم تصنيف الشركات طبقا لمصفوفة التقييم التالية لتحديد مدي جاهزية الشركة لمواجهة تهديدات الامن السيبراني وفاعلية الإجراءات لديها عبر معرفة موقع الشركات بالنسبة لمستويات التقييم الخمسة التم تم اعدادها وهي كالتالي :

جدول رقم 7: معايير تحديد مستوي الشركات

المستوى	أبرز الخصائص
مستدام (Sustainable)	تبني أطر دولية + ميزانية + خطة DRP + أدوات متقدمة
مدار (Managed)	ميزانية مخصصة + تقييم دوري + سياسات واضحة
منظم (Organized)	سياسات موثقة + مسؤولية محددة + التزام جزئي بالقانون
تفاعلي (Reactive)	استجابة فقط عند وقوع الحوادث
متدني (Initial)	غياب السياسات والأدوات والميزانية

5.5.1- منهجية التصفية والوزن النسبي(The Filter & Weighting)

في هذا التقييم، قمنا باستبعاد "أسئلة الرأي" (مثل: هل تعتقد أن التهديدات زادت؟) وركزنا على 16مؤشراً إجرائياً .استخدمنا "طريقة الأوزان المرجحة" حيث تم تصنيف الأسئلة إلى 3 محاور تنفيذية:

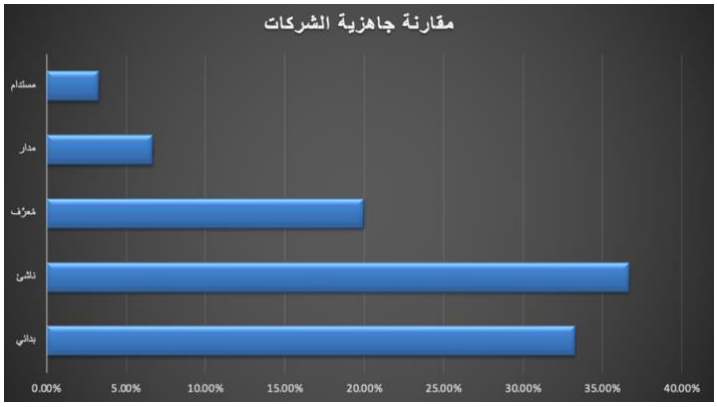
1. **محور الامتثال القانوني (Compliance)** : س10، س11، س13، س15، س17.
2. **محور الجاهزية التقنية Technical)** : س12، س18، س19، س21، س23، س24، س26، س27.
3. **محور الحوكمة والموارد (Governance)** : س14، س22، س30، س31.

5.5.2- نتائج تصنيف الشركات بناءا على معايير التقييم

تصنيف النضج	حالة الجاهزية الإجرائية والتقنية	عدد الشركات	النسبة المئوية
بدائي	شركات تعاني من انكشاف أمني كامل، وتفتقر لأي سياسات أو ميزانيات، واعتمادها الكلي على ردود الفعل اللحظية.	10	%33.30
ناشئ	شركات تمتلك بعض الأدوات التقنية والبرمجيات، لكنها تفتقر للتوثيق الإجرائي والمنهجية، وتعتمد على مجهودات فردية غير منتظمة.	11	%36.70
مُعرَّف	شركات لديها سياسات مكتوبة والتزام بالتشريعات القانونية، لكنها تفتقر للموارد المالية والكفاءات البشرية اللازمة للتفعيل المستمر.	6	%20.00
مدار	شركات تقوم بعمليات التدقيق والمراقبة الدورية للأنظمة، ولديها هيكل إداري تقني وميزانية مخصصة (جزئياً) للأمن.	2	%6.70
مستدام	شركات وصلت لمرحلة الحماية الاستباقية الشاملة، مع تكامل تام بين الموارد المالية والبشرية والتقنيات الذكية.	1	%3.30

القراءة التحليلية لنتائج ترتيب العينة

1. **التركيز في الفئات الدنيا** :يلاحظ أن الكتلة الحرجة من الشركات **(70%)** تقع في فئتي" **بدائي** "و"**ناشئ**"، مما يشير إلى أن أغلب الشركات التكنولوجية الناشئة في القاهرة ما زالت تعمل خارج إطار الحماية المنهجية، رغم وعيها النظري بالمخاطر.
2. **عائق العبور للفئات العليا** :الفجوة الكبيرة بين فئة" **مُعرَّف** "وفئة" **مدار** "تؤكد أن العائق ليس "قانونياً" أو "ورقياً"، بل هو عائق "تشغيلي ومالي" يمنع الشركات من تحويل السياسات المكتوبة إلى إجراءات مدارة ومراقبة تقنياً.



3. **ندرة النموذج المستدام** :بقاء شركة واحدة فقط في فئة" **مستدام** "يثبت أن الوصول للنضج الكامل يتطلب استثمارات تفوق القدرات الحالية لغالبية الشركات الصغيرة والمتوسطة، مما يجعلها دائماً في حالة "تبعية أمنية" أو انتظار لوقوع التهديد قبل التحرك.

5.6- دراسة الحالة

اسم الشركة: (X) – تم حجب اسم الشركة

5.6.1- مبررات اختيار الشركه : تم اختيار شركة (X) كنموذج تطبيقي لتعميق نتائج الدراسة الميدانية، حيث تمثل الشركة شريحة "الشركات المتوسطة" (Medium Enterprises) في قطاع تكنولوجيا المعلومات بالقاهرة (100 موظف). وتأتي أهمية هذه الحالة من كونها تمتلك بنية تحتية تقنية "هجينة" (Hybrid Infrastructure) تجمع بين الخوادم الداخلية والخدمات السحابية، ومع ذلك فقد سجلت إخفاقات أمنية حقيقية توفر مادة غنية لتحليل الفجوة بين "الاستثمار التقني" و"الحوكمة الإدارية".

التوصيف الفني لبيئة العمل قبل الحوادث من خلال المقابلة المتعمقة مع المسؤول الفني للبيانات، تبين أن الشركة تعتمد على مزيج تقني يشمل:

- إدارة البيانات: خوادم داخلية (On-premise) لإدارة البرمجيات الإدارية، وخوادم سحابية (Cloud) لإدارة العمليات الخارجية.
- النسخ الاحتياطي: وجود نظام نسخ احتياطي مزدوج (محلي وسحابي).
- الوسائل الدفاعية: الاعتماد الكلي على التجهيزات الصلبة (Hardware) مثل أجهزة الجدار الناري (Firewalls).
- الحوكمة: غياب تام للسياسات المكتوبة (Formal Policies)، والاعتماد على الخبرة الفنية الفردية دون وجود إطار تنظيمي موحد.

5.6.2- تحليل الحوادث السيبرانية المرصودة.

تعرضت الشركة لثلاثة أنماط مختلفة من الهجمات الناجحة، يحللها الباحث فيما يلي:

أ. حادثة اختراق السنترال الدولي (Toll Fraud): حيث تم استغلال ثغرة في السنترال الداخلي لإجراء مكالمات دولية باهظة الثمن.

- سبب الفشل: ضغط الإدارة لتشغيل تطبيقات المكالمات عبر الإنترنت أدى لتعطيل الجدار الناري يدوياً لتسهيل الربط، مما خلق "ثغرة مقصودة".
- طريقة الاكتشاف: تم الاكتشاف عبر جهة خارجية (شرطة الاتصالات) نتيجة ارتفاع الفاتورة، مما يشير إلى فشل ذريع في وظيفة "الاكتشاف" (Detect) الداخلية.

ب. هجوم فدية على أنظمة المراقبة (Ransomware): تشفير كامل لتسجيلات كاميرات المراقبة على الخوادم.

- سبب الفشل: ضعف تأمين أجهزة الإنترنت الأشياء (IoT) المتصلة بالشبكة.
- طريقة الاكتشاف: اكتشاف عرضي من قبل مهندس المتابعة وليس عبر نظام إنذار مؤتمت.

ج. التهديد الداخلي (Insider Threat): قيام موظف حسابات بتخريب وتشفير البيانات المالية قبيل مغادرته الشركة.

- سبب الفشل: غياب سياسة "إدارة الصلاحيات" (Access Management) وعدم وجود إجراءات تقييد الوصول الفوري عند انتهاء العلاقة التعاقدية.

5.6.3 - تحليل النتائج دراسة الحالة

بناءً على الوقائع السابقة، يمكن استخلاص النتائج

1. سجلت الدراسة فشلاً حاداً في هذا المحور؛ حيث تغلبت "الرغبات التشغيلية" وضغوط الإدارة على "المتطلبات الأمنية". غياب السياسات المكتوبة جعل قرار تعطيل الجدار الناري قراراً فردياً غير خاضع للمساءلة.
2. تفتقر الشركة لعملية "تحديد المخاطر" مسبقاً، حيث تم التعامل مع كل هجوم كفعل مفاجئ دون وجود سجل مخاطر (Risk Register) يتوقع هذه السيناريوهات.

3. رغم توفر الأدوات (Firewalls)، إلا أن "إدارة الهوية والوصول" كانت الغائب الأكبر، مما سمح للموظف الداخلي بالتخريب دون عوائق.
4. أثبتت الحالة أن الشركة "عمياء" تقنياً؛ فالاكتشاف إما خارجي (شرطة الاتصالات) أو عرضي (بالصدفة)، مما يرفع من "زمن البقاء" (Dwell Time) للمهاجم داخل الشبكة.
5. كانت الاستجابة "بترية" (Isolation) عبر فصل الأنظمة عن الإنترنت كلياً، وهو ما يمثل فشلاً في استمرارية الأعمال. كما أن النسخ الاحتياطية لم تكن فعالة في تقليل زمن التوقف نتيجة غياب "خطة استعادة" مختبرة.

5.6.4- تقييم أداء الإدارة والتعلم المؤسسي

تتمثل النتيجة الأكثر أهمية في هذه الدراسة في "رد الفعل الإداري" بعد الأزمة:

- إهمال التدريب: لم يتم تفعيل أي برامج توعية للموظفين (Security Awareness) رغم مرور سنوات على الحوادث، مما يعني بقاء "الثغرة البشرية" قائمة.
- جمود الميزانية: لا تزال الإدارة تنظر للإنفاق على الأمن السيبراني كعبء مالي وليس كحماية للأصول الرقمية، رغم جودة دخل الشركة.
- إحلال الثقة محل الكفاءة: لم تتوجه الشركه للاستعانه بالمتخصيصين او بالتعاقد مع طرف ثالث للفحص والتأمين وظل الاعتماد علي موظف كفء في اعمال تكنولوجيا المعلومات.

خلاصة دراسة الحالة:

تؤكد حالة شركة (X) أن امتلاك "العتاد التقني" دون "إطار حوكمة ومتابعة" هو استثمار غير محمي. إن التحول من إدارة الأزمات بـ "الصدفة" إلى إدارتها بـ "المنهجية" (مثل إطار NIST) هو الضرورة التي تفرضها هذه الدراسة لضمان استدامة الشركات المتوسطة في بيئة الأعمال المصرية.

5.7- مقارنة نتائج الدراسة بالتقارير العالمية

لا يمكن فهم واقع الأمن السيبراني للشركات الصغيرة والمتوسطة في القاهرة بمعزل عما يحدث في العالم. لذلك قارنا نتائج البحث بأحدث التقارير الدولية الصادرة في 2025 و2026. ويمكن أبراز النقاط المشتركة والمختلفة فيما يلي:

1. **الثغرة البشرية هي الأكبر عالمياً** أظهر البحث أن هجمات التصيد الاحتيالي (Phishing) هي الأكثر شيوعاً. وهذا يتفق تماماً مع تقرير **Verizon DBIR 2025**، الذي أكد أن **60%** من الاختراقات العالمية تنطوي على خطأ بشري (مثل النقر على روابط مزيفة أو إعطاء بيانات.
2. **فجوة كبيرة بين الشركات الكبيرة والصغيرة** أثبت تحليل النتائج أن الشركات الصغيرة جداً (أقل من 20 موظف) تعاني أكثر بسبب نقص الميزانية والأدوات .هذا يتطابق مع تقرير **WEF Global Cybersecurity Outlook 2026**، الذي حذَّر من الفجوة السيبرانية المتزايدة بين الشركات الكبيرة التي تتقدم بسرعة و الشركات الصغيرة والمتوسطة التي تتخلف بسبب نقص الموارد والخبرات.
3. **معظم الشركات لم تصل بعد إلى مستوى جيد** رغم الوعي النظري العالي، وجدنا أن **70%**من الشركات في المستويين الأدنى بدائي وناشئ .(هذا يتطابق مع **مؤشر Cisco Cybersecurity Readiness Index 2025)**، الذي أظهر أن **70%**من الشركات العالمية ما زالت في المراحل الأولى (مبتدئة أو جزئية)، وأن نسبة الشركات المتقدمة جداً لا تتجاوز **4%** فقط .

4. **الامتثال للقوانين** : أظهرت الدراسة أن "وجود قانون ملزم" هو أكبر دافع للالتزام (29%)، لكن التنفيذ الفعلي ما زال متوسطاً .يتفق ذلك مع تقرير **IBM Cost of a Data Breach 2025**، الذي أوضح أن التشريعات الجديدة تزيد التكاليف الأولية على الشركات الصغيرة، وأنها تحتاج إلى حوافز مالية أو نماذج مبسطة حتى لا تتعثر.

الخلاصة :تشير نتائج البحث ان الحالة بالشركات الصغيرة والمصرية ليست استثناءً، بل تعكس واقعاً عالمياً. وان أبرز التحديات تتركز في ضعف الدفاعات البشرية و نقص الموارد وصعوبة التنفيذ العملي رغم الوعي النظري. وهذا يعطي نتائج البحث مصداقية ويؤكد الحاجة إلى حلول عملية مبسطة ومنخفضة التكلفة.

الخاتمه

الخلاصة: تمثل الهجمات السيبرانية في العصر الرقمي الحالي تهديداً وجودياً لاستمرارية الأعمال، حيث تتجاوز أضرارها الجوانب التقنية المحدودة لتشمل السمعة المؤسسية والاستقرار المالي للشركات. واستناداً إلى ما تم رصده وتحليله في الفصول السابقة من فجوات في بيئة الشركات التكنولوجية بالقاهرة، يأتي هذا الفصل ليكون الجسر الرابط بين "الواقع المرصود" و"الحل المأمول."
يهدف هذا الفصل إلى بلورة النتائج النهائية للدراسة وتحويلها إلى قيمة مضافة من خلال تقديم إطار عملي مقترح يرتكز على معايير (NIST 2.0)، ويوضح كيفية الانتقال بالشركات من نموذج "الدفاع التقليدي" القائم على رد الفعل إلى نموذج "الحوكمة السيبرانية" الاستباقي. كما يستعرض الفصل مجموعة من التوصيات الإجرائية الموجهة لصناع القرار والجهات المعنية، وصولاً إلى آفاق جديدة للبحوث المستقبلية التي تدعم مرونة هذا القطاع الحيوي.

6.1- أبرز نتائج الدراسة الميدانية

6.1.1- واقع النضج والجاهزية السيبرانية كشفت الدراسة عن فجوة حادة في النضج السيبراني؛ حيث تقع 70% من الشركات في المستويات الأدنى (33.3% في المستوى "البدائي" و36.7% في المستوى "الناشئ"). تعمل غالبية هذه الشركات في بيئة منكشفة أمنياً، تفتقر للسياسات الموثقة وأنظمة الإنذار المبكر، مما يجعل استجابتها للتهديدات لحظية وغير منهجية.

6.1.2- مسببات التهديدات وأنماط الاختراق أظهرت النتائج تفوق الثغرات السلوكية والإجرائية على الثغرات التقنية. يتصدر "ضعف الوعي الإجرائي لدى الموظفين" المرتبة الأولى كأهم مسبب للمخاطر. ونتيجة لذلك، كانت هجمات الهندسة الاجتماعية (Phishing) الأكثر نجاحاً في اختراق الشركات، مما يؤكد أن التركيز على الأدوات التقنية دون بناء منظومة سلوكية يبقي الشركات عرضة للاختراق.

6.1.3- فجوة الوعي التشغيلي والتعثر المالي سجلت الإدارة العليا وعياً نظرياً مرتفعاً جداً (4.7)، بينما انخفض المتوسط المرجح للتخصيص المالي والتدريب الفعلي إلى (2.8). هذا التباين يعكس "مفارقة الوعي السلبي"، حيث يكمن العائق الأساسي في الجانب التمويلي والإداري وليس المعرفي.

6.1.4- الهيكل التنظيمي وإدارة الأزمات

- تداخل المهام: يُسند الأمن السيبراني إلى مدير تكنولوجيا المعلومات (IT Manager) في 46.67% من الشركات، مما يؤدي إلى غياب فصل السلطات وإهمال الجانب الأمني.

- عشوائية الاستجابة: يتم التعامل مع الحوادث بـ"البتر التقني" غير الممنهج (مثل فصل الأنظمة كلياً) بدلاً من بروتوكولات التعافي، مما يضاعف الخسائر التشغيلية.

الخلاصة البحثية :تعكس الشركات المبحوثة نضجاً نظرياً مرتفعاً يقابله عجز إجرائي حاد، مما يكرس حالة من الهشاشة الأمنية ويمنع الشركات الناشئة من الانتقال من المستويات البدائية إلى المستويات المدارة والمستدامة.

6.2- مناقشة وتفسير النتائج

تكشف نتائج الدراسة الميدانية عن أداء ضعيف نسبياً للشركات التكنولوجية الصغيرة والمتوسطة في تقييم فاعلية الإجراءات الوقائية ضد التهديدات السيبرانية. فعلى الرغم من تسجيل المحور الأول (إدراك التهديدات) أعلى متوسط (4.47) بانحراف معياري منخفض يعكس وعياً نظرياً مرتفعاً، إلا أن هذا الوعي لم ينعكس على مستوى التنفيذ العملي، حيث سجلت محاور الجاهزية والسياسات (3.8) والالتزام بالتشريعات (3.5) متوسطات متوسطة إلى منخفضة.

ويفسر الباحث هذا الأداء المتواضع بثلاثة عوامل جوهرية:

1. **محدودية فاعلية الإجراءات الوقائية** :أظهرت النتائج أن 70% من الشركات ما زالت في المستويين «البدائي» و«الناشئ»، مما يعني أن معظم الإجراءات الوقائية الحالية (مكافحة الفيروسات والجدران النارية) هي إجراءات دفاعية سطحية ورد فعلية، ولا تلبي متطلبات الحماية الاستباقية أو التعافي السريع.
2. **الفقر المالي والتخصصي** :أكد تحليل الارتباط القوي ($r = 0.831$) بين توفر الميزانية وتطبيق الأدوات التقنية أن نقص الموارد يُعد العائق الأكبر أمام رفع فاعلية الإجراءات الوقائية، خاصة في الشركات الصغيرة جداً التي سجلت أدنى مستوى نضج (37.7%).
3. **تداخل المهام وعدم وجود حوكمة أمنية** :تركز المسؤولية الأمنية على مدير تكنولوجيا المعلومات بنسبة 46.67%، مما يؤدي إلى غياب فصل السلطات الرقابية ويجعل الإجراءات الوقائية مرهونة بالمبادرات الفردية بدلاً من النظم المؤسسية المنظمة.

وبالتالي، يرى الباحث أن **فاعلية الإجراءات الوقائية الحالية لا تزال محدودة جداً**، وأن الشركات تمتلك وعياً نظرياً جيداً بالمخاطر لكنها أسيرة «الهشاشة الإجرائية» التي تحول دون الانتقال إلى مستويات النضج المدارة والمستدامة. وهذا يعزز فرضية الدراسة بأن التحدي الحقيقي ليس في «المعرفة» بل في «القدرة على التنفيذ»، ويستدعي تدخلاً تشريعياً ومؤسسياً يراعي حجم الشركات وقدراتها (حلول منخفضة التكلفة، برامج تدريبية مخصصة، وشراكات تمويلية)

6.3- الإطار المقترح للشركات الصغيرة والمتوسطة بالقاهرة.

تم تصميم هذا الإطار كمجموعات مترابطة تشكل دورة كاملة قابلة للتطبيق العملي في الشركات الصغيرة والمتوسطة.

الإطار يغطي **6 مجموعات رئيسية** فقط (ليكون سهل التنفيذ وغير معقد)، وكل مجموعة تحتوي على 4-5 عمليات أساسية مترابطة مع الآخرين ومتوافقة مع تتوافق مع(NIST Identify + ISO 27001 A.8 + SOC 2 Security) :

مجموعة -1- جرد وإدارة الأصول(Asset Inventory & Management)

- جرد الأصل(Asset Inventory)
- متابعة الأصل(Asset Monitoring & Tracking)
- إعدام الأصل(Secure Asset Disposal)
- حركة الأصل(Asset Movement & Change Management)
- تصنيف الأصل(Asset Classification & Labeling)

مجموعة 2- إدارة المخاطر والحوكمة(Risk & Governance Management)

- تحديد المخاطر(Risk Identification & Assessment)
- معالجة المخاطر(Risk Treatment & Acceptance)
- سياسات الحوكمة(Policy & Leadership Commitment)
- تقييم الامتثال القانوني(Legal & Regulatory Compliance)

مجموعة 3- حماية وتأمين البيئة(Protection & Safeguarding)

- التحكم في الوصول(Access Control & Least Privilege)
- التشفير والنسخ الاحتياطي(Encryption & Backup)
- الحماية من البرمجيات الضارة والتحديثات(Malware Protection & Patch Management)
- التكوين الآمن(Secure Configuration & Hardening)

مجموعة 4- الكشف والمراقبة(Detection & Monitoring)

- تسجيل الأحداث والمراقبة(Logging & Continuous Monitoring)
- كشف التهديدات(Threat Detection & Anomaly Alerts)
- فحص الثغرات الدوري(Vulnerability Scanning)
- مراقبة الشبكة والتطبيقات(Network & Application Monitoring)
- تقارير الكشف المبكر(Early Warning Reporting)

مجموعة 5- الاستجابة والتعافي(Response & Recovery)

- الاستجابة للحوادث(Incident Response Plan)
- التحقيق والاحتواء(Investigation & Containment)
- التعافي من الكوارث(Disaster Recovery & Business Continuity)
- الإبلاغ والإخطار(Breach Notification & Reporting)
- الدروس المستفادة(Post-Incident Review & Lessons Learned)

مجموعة 6- التدريب والوعي والتحسين المستمر (Training, Awareness & Continuous Improvement)

- برامج التوعية والتدريب(Security Awareness Training)
- تقييم الكفاءات البشرية(Competence & Skill Assessment)
- إدارة التغيير والتحسين(Change Management & Improvement)
- التدقيق الداخلي(Internal Audit)
- قياس الأداء والمؤشرات(KPI Measurement & Reporting)

كيفية الترابط بين المجموعات:(Interconnection)

- تبدأ المجموعة 1 (الجرد) بتغذية المجموعة 2 (المخاطر).
- تنتقل المخاطر إلى المجموعة 3 (الحماية).
- تراقب المجموعة 4 (الكشف) كل شيء.

- تفعّل المجموعة 5 (الاستجابة) عند الحاجة.
- تغذي المجموعة 6 (التدريب) كل المجموعات بالتحسين المستمر .

6.4- توصيات الدراسة

بناءً على تحليل الفجوات بين الوعي والممارسة، وفي سبيل تحويل "الوعي السلبي" إلى التزام مؤسسي فعال، تقدم الدراسة التوصيات التالية مقسمة على أربعة مسارات تكاملية:

6.4.1- التوصيات المؤسسية والتشريعية (الدور الحكومي)

- الإسراع في إصدار اللائحة التنفيذية للقانون رقم (151 لسنة 2020) قانون حماية البيانات الشخصية لتحديد المسارات الإجرائية والعقوبات.
- اشتراط الحصول على شهادة اعتماد سيبراني رسمية كمصوغ أساسي لتسجيل الشركات، أو تجديد تراخيصها، أو التعاقد مع الجهات الحكومية والمشاريع القومية.
- قيام الجهاز القومي لتنظيم الاتصالات (NTRA) بتوفير حوافز تقنية، مثل تراخيص البرمجيات الأصلية بأسعار مدعومة للشركات الملتزمة بمعايير الأمن السيبراني.

6.4.2- التوصيات الاستراتيجية والمالية (أصحاب الأعمال)

- إلزام الشركات بتخصيص نسبة لا تقل عن 1%من إجمالي الميزانية السنوية لدعم التطور التكنولوجي والأمن السيبراني تسجل ضمن القوائم الماليه السنويه.

6.4.3- التوصيات التقنية والابتكارية (منصة الامتثال الذكية)

- إنشاء منصة رقمية تفاعلية تعمل كطرف ثالث معتمد، تعتمد على الذكاء الاصطناعي لتقييم مستندات وسياسات الشركات آلياً دون تدخل بشري.
- توفير خدمات أمنية مباشرة عبر المنصة (مثل إدارة كلمات المرور، المصادقة الثنائيةMFA ، ومحاكاة الاختراق) لتسهيل الامتثال للشركات التي تفتقر للخبرات الفنية.
- توفير مستوى "خدمي/توعوي" مجاني لجذب الشركات، ومستوى "اعتماد" مدفوع (برسوم بسيطة) للحصول على الشهادات الرسمية.

6.4.4- توصيات بناء القدرات البشرية (التدريب الهجين)

- التوقف عن الفصل التقليدي بين موظف الـ IT ومسؤول الأمن في الشركات الصغيرة، والبدء في تقديم دورات تدريبية تجمع بين مهارات الإدارة (Operations) والحماية(Security) .
- تصميم برامج تدريبية تركز على ثلاث مهارات عملية لا غنى عنها:

الحماية :(Protect) تأمين الأصول وإدارة الهوية.

الاستجابة :(Respond) كيفية التعامل مع الاختراق فور وقوعه.

التعافي :(Recover) استعادة البيانات وضمان استمرارية العمل.

المراجع

أولاً: المراجع العربية

1. إبراهيم، يوسف، عيد. (2022). الأمن السيبراني والنظافة الرقمية. *المجلة المصرية لعلوم المعلومات*.
https://journals.ekb.eg/article_265428_ca3307f7b4f2589bfe504391b6dc2586.pdf
2. خشبة، الريس وآخرون. (2021). *الأبعاد التنموية والاستراتيجية للأمن السيبراني ودوره في دعم الاقتصادات الرقمية والمشفرة: مسارات التجربة المصرية في ضوء التجارب العالمية*. سلسلة قضايا التخطيط والتنمية. معهد التخطيط القومي.
3. جمهورية مصر العربية (2020). *قانون رقم 151 لسنة 2020 بشأن حماية البيانات الشخصية*. الجريدة الرسمية، العدد 33 مكرر (ب).
4. المجلس الأعلى للأمن السيبراني. (2023). الاستراتيجية الوطنية للأمن السيبراني لجمهورية مصر العربية (2023-2027). الجهاز القومي لتنظيم الاتصالات.
https://egcert.eg/wpcontent/uploads/2024/02/Publications_1412024000_ar_National_Cybersecurity_Strategy_2023_2027.pdf

ثانياً: المراجع الأجنبية

1. Organization for Economic Co-operation and Development. (2025). *SME and entrepreneurship policy in Egypt*. https://doi.org/10.1787/195d9c43-en
2. Mordor Intelligence. (2025). *Egypt ICT market: Size, share & industry analysis*.. https://www.mordorintelligence.com/industry-reports/egypt-ict-market
3. Calvo-Manzano, J. A., García-García, J. A., San Feliu Gilabert, T., & Cuevas Agustín, P. (2025). CyberESP: An integrated cybersecurity framework for SMEs. *Journal of Software: Evolution and Process*, *37*(9), Article e70050. https://doi.org/10.1002/smr.70050
4. IBM Security. (2025). *Cost of a data breach report 2025.* IBM Corporation. https://www.ibm.com/reports/data-breach
5. Mkhulisi, N. (2025). *Cybersecurity skill requirements for small and medium-sized enterprises' employees* [Master's dissertation, University of Johannesburg]. University of Johannesburg Research Portal. https://ujcontent.uj.ac.za/esploro/outputs/graduate/Cybersecurity-skill-requirements-for-small-and/9957588707691
6. ENISA. (2024). *ENISA threat landscape 2024.* European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
7. Ministry of Communications and Information Technology**.** (2024)**.***National cybersecurity report of Egypt 2024.* https://mcit.gov.eg
8. Alexandria Journal of Administrative and Economic Research. (2024). *The impact of cybersecurity risk management disclosure on investment decisions in small and medium-sized enterprises: An empirical study on companies listed on the Egyptian Stock Exchange.* https://aljalexu.journals.ekb.eg/article_345478.html
9. Hoong, Y., & Rezania, D. (2024).*Balancing talent and technology: Navigating cybersecurity and privacy in SMEs. Telematics and Informatics Reports, 14*, 100179. https://doi.org/10.1016/j.teler.2024.100179

11. U.S. Department of Commerce, International Trade Administration. (2023). *Egypt: Digital economy.* https://www.trade.gov/country-commercial-guides/egypt-digital-economy
12. Verizon Business. (2023). *2023 data breach investigations report (DBIR).* https://www.verizon.com/business/resources/reports/dbir/2023-dbir.pdf
13. Erdogan, G. (2023). *Cybersecurity awareness and capacities of SMEs. International Journal of Cybersecurity Studies, 6*(2), 112–130.
14. ENISA. (2023). *ENISA threat landscape report 2023.* European Union Agency for Cybersecurity.
15. Cisco Systems Inc. (2023**).** *Annual cybersecurity report 2023.* Cisco Talos Intelligence Group. https://www.cisco.com
16. Tam, T., Rao, A., & Hall, J. (2021). *The good, the bad and the missing: A narrative review of cybersecurity implications for Australian small businesses.* arXiv. https://arxiv.org/abs/2109.00733
17. Bada, A., & Nurse, J. R. C. (2021). *The cybersecurity awareness gap in small and medium-sized enterprises. Computers & Security, 105*, 102248. https://doi.org/10.1016/j.cose.2020.102248
18. International Finance Corporation. (2012)**.** *Interpretation note on small and medium enterprises and small mid-cap companies.* World Bank Group. https://www.ifc.org/content/dam/ifc/doc/mgrt/interpretationnote-sme-2012.pdf
19. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST Special Publication). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29
20. International Organization for Standardization. (2022 .(*Information security, cybersecurity and privacy protection — Information security management systems — Requirements*)ISO/IEC Standard No. 27001 .(https://www.iso.org/standard/27001
21. American Institute of Certified Public Accountants. (2017). *Trust services criteria for security, availability, processing integrity, confidentiality, and privacy*. AICPA. https://www.aicpa.org
22. National Institute of Standards and Technology. (2017). *An Introduction to Information Security* (NIST Special Publication 800-12 Rev. 1). U.S. Department of Commerce.
23. EG-CERT. (2024). *Egypt classified in Tier 1 according to ITU Global Cybersecurity Index*. National Telecom Regulatory Authority. https://www.tra.gov.eg/en/egypt-classified-in-tier-1-according-to-itu-global-cybersecurity-index/
24. INTERPOL. (2025). *Africa Cyberthreat Assessment Report 2025*. https://www.interpol.int/content/download/23094/file/INTERPOL_Africa_Cyberthreat_Assessment_Report_2025.pdf
25. Mordor Intelligence. (2026). *Egypt cybersecurity market size & share analysis*. https://www.mordorintelligence.com/industry-reports/egypt-cybersecurity-market
26. National Telecom Regulatory Authority (NTRA). (2022). *Egypt among 20 most vulnerable countries to cyber attacks*. Daily News Egypt. https://www.dailynewsegypt.com/2022/09/27/egypt-among-20-most-vulnerable-countries-to-cyber-attacks-ntra/
27. Positive Technologies. (2025). *Cyberattacks on Egypt's infrastructure in 2024*. https://global.ptsecurity.com/analytics/cyberattacks-on-egypt-s-infrastructure-in-2024
28. Verizon. (2025). *2025 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/

الملاحق

الاستبيان – أولا اسئله بنظام ليكارت

المحور	رقم السؤال	مضمون السؤال	غير موافق بشده	غير موافق	محايد	موافق	موافق بشده
المحور الأول: إدراك التهديدات السيبرانية ونقاط الضعف	س4	هل تعتقد ان جميع الشركات معرضة لتهديدات سيبرانية بغرض التخريب او السرقه او الابتزاز او ايقاف الاعمال او التجسس؟					
	س5	هل تعتقد انه يمكن التجسس عليك او سرقة بيانات هامه لدي الشركه او غير ذلك من الاثار السلبيه للهجمات السيبرانيه - دون ان تكتشف ذلك؟					
	س7	هل تعتقد أن الاعتماد المتزايد على التكنولوجيا في العمليات اليومية مع ضعف الوعي الامني لدى الكوادر البشرية يمثل التهديد الرئيسي لاحتمالية التاثر سلبيا بهجمات سيبرانيه؟					
	س16	هل الإفصاح (الإعلان) عن التعرض لهجمات سيبرانيه ناجحه قد يؤثر علي سمعة الشركه او بيئة اعمال الشركه – وبالتالي يتم التعامل مع الهجمات بسريه تامه واخفاء تاثيرها؟					
المحور الثاني: الالتزام بالتشريعات الوطنية (قانون 2020/151)	س9	ما مدي إلمامك (معرفتك) بالمبادرات الوطنيه والقوانين والتشريعات المصريه لتنظيم الامن السيبراني؟					
	س10	ما مدي التزام شركتك بالقوانين والتشريعات المصرية المنظمه لحماية البيانات الشخصية وإجراءات الامن السيبراني؟					
	س14	تواجه الشركه حاليا صعوبات تنظيمية أو مالية تحول دون الالتزام الكامل بالتشريعات الوطنية للأمن السيبراني؟					
	س15	هل توافق علي ان الالتزام بالتشريعات الوطنية، خاصة قانون 2020/151، سوف يساعد في تقليل مخاطر الانتهاكات السيبرانية في الشركات الصغيرة والمتوسطة؟					
المحور الثالث: الجاهزية والسياسات وآليات المتابعة	س6	هل تتفق مع التقارير التي تفيد ان الشركات المصرية (الصغيره والمتوسطه) مستعده - بدرجه كبيره- لمواجهة أي تهديدات سيبرانية معقده؟					
	س12	هل يتم تطبيق سياسات وتعليمات صارمه بالشركه لتعزيز الامن السيبراني؟					
	س20	هل توافق عل ان احد السياسيات التي يجب تطبيقها بالشركه هو الاعتماد علي البرامج الاصليه فقط في اعمال الشركه؟ (تم نقله هنا لتعزيز الثبات)					
	س21	هل يوجد ميزانيه مخصصه سنويا لتحديث برامج الفيروسات وتراخيص انظمة الجدار الناري وشراء الاصدارات الحديثه من التطبيقات والبرامج؟					

	س24	تقييم/مراجعة الأمن السيبراني داخل الشركة دورياً – شيء ضروري للشركه؟						
	س26	لدي توجد خطة معتمدة لاستعادة البيانات (Disaster Recovery) في حال وقوع اختراق او تلف لها؟						
المحور الرابع: تحديات تبني الأطر الدولية ومسارات التطوير	س22	هل تري ان التدريب الدوري لزيادة الوعي داخل الشركه هام جدا لمواجهة الهجمات السيبرانيه؟						
	س30	تواجه الشركات تحديات في تبني واتباع الأطر الدولية (Framework) للأمن السيبراني بسبب نقص الموارد و الكفاءات البشرية؟						
	س31	تواجه الشركات تحديات في تبني الأطر (Framework) الدولية للأمن السيبراني بسبب نقص الموارد - المالية -؟						

– ثانيا : أسئلة الاختيار المتعدد

س1: اسم الشركة	
س2: كم عدد الموظفين؟	■ 1 to 5 ■ 5 to 20 ■ 20-100 ■ 100-250
س3 : ما هو نشاط عمل الشركه؟	■ خدمات تكنولوجيه ■ توريدات تكنولوجيه ■ استشارات ■ مقاولات ومشاريع تكنولوجيه ■ اخري
س8: من وجهة نظرك - ما هي الأسباب التالية التي يمكن أن تؤدي إلى اختراقات أمنية حقيقية بالشركة؟	■ انخفاض وعي الموظفين ■ استخدام برامج غير اصليه ■ عدم تحديث البرامج ■ غياب المتخصصين المؤهلين أو قسم مستقل للأمن السيبراني. ■ عدم وجود ادوات التامين المناسبة ■ استخدام الموظفين لأجهزتهم الشخصية ■ الاعتماد على أطراف خارجية أو خدمات سحابية دون اشتراطات أمنية كافية. ■ غياب نظام فعال للنسخ الاحتياطي أو عدم اختباره دورياً. ■ عدم وجود سياسات وإجراءات أمنية مكتوبة أو خطة للاستجابة للحوادث. ■ اخري ■ لا اعلم
س11 : من المسؤول عن متابعة الالتزام بحماية البيانات الشخصية للقوانين والتشريعات المصرية؟	■ الشئون القانونيه بالشركة. ■ الاداره التنفيذيه / المدير العام. ■ مهندس الامن السيبراني اوIT ■ لم اسمع باي قوانين سابقا ■ لا يوجد احد مسئول
س12 – هل يتم تطبيق سياسات صارمه بالشركه لتعزيز الامن السيبراني ؟	■ لا يوجد ■ لا اعلم ■ ربما ■ بعض السياسات ■ نعم توجد سياسات صارمه

س13: أياً من السياسات (التعليمات) التشغيلية التالية تطبقها في شركتك؟	■ سياسة تحديد صلاحيات الوصول الي البيانات كل موظف ■ فصل وظيفة الامن السيبراني عن ادارة شبكة المعلومات ■ سياسة التحديثات البرمجية(Patch Management Policy) ■ استخدام اجهزة الشركه فقط ومنع استخدام الاجهزه الشخصيه الخاصه بالموظفين ■ تغيير الباسورد باستمرار للسيرفرات وانظمة الواي فاي وصلاحيات الموظفين ■ الزامية استخدام المصداقية الثنائية في جميع البرامج خاصة علي الانترنت Two-factor-Authentication ■ سياسة الاستجابة للحوادث والايميلات المشبوهه(Incident Response Policy) ■ منع استخدام usb الشخصيه او اي ادوات حفظ بيانات خارجيه علي شبكات وانظمة الشركه ■ سياسة التدريب والتوعية الدورية(Security Awareness Training) ■ لا توجد اي سياسه معتمده تطبق علي كل المتعاملين بالشركه ■ سياسات اخري
س17: حاليا إذا تم اكتشاف أن هناك محاولة اختراق أمني سيبراني بأحد الطرق - مثل ايميلات الاحتيال phishing - فما هي الإجراءات التي تتخذ؟	■ ابلاغ مسئول امن المعلومات بالشركه ■ ابلاغ قسم الموارد البشريه ■ ابلاغ مدير IT ■ ازسال ايميلات لجميع الموظفيين للتحذير ■ ضبط انظمة الامن والحمايه للتعامل مع هذا الاختراق ومنعه مستقبلا ■ لا يتم اتخاذ أي اجراء - ويتم اهمال الحدث الأمني ■ اخري ■
س18: من المسؤول عن حماية البيانات من التلف أو السرقة أو الاستخدام غير الآمن بالشركة؟	■ مسئول الامن السيبراني بالشركه ■ مهندس ادارة شبكة المعلوماتIT Manger/Engineer ■ تم التعاقد مع شركه خارجيه للتامين السيبراني ■ نعتمد علي موظف بالشركه له مهارات تكنولوجيه ■ كل موظف مسئول عن بياناته ■ لا يوجد
س19: ما هي الأدوات والحلول التكنولوجية المعتمدة حالياً داخل الشركة لتعزيز الأمن السيبراني وحماية الأصول الرقمية؟	■ انظمة الجدار الناريFirewall ■ برامج الحماية من الفيروساتAnti-Virus ■ برامج اكتشاف الاختراقات(IDS) Intrusion detection system ■ برامج منع الاختراقات(IPS) Intrusion Prevention system ■ تفعيل خواص Domain Controller للتحكم الكامل ■ تحديثات الأنظمة التلقائية(Automated Patching) ■ استخدام انظمة حماية وحفظ البيانات(local/cloud) backup solution ■ استخدام برامج تشفير البيانات - وتشفير نقل البيانات ■ برامج إدارة كلمات المرور(Password Managers) ■ استخدام الشبكات الخاصة الافتراضية(VPN) ■ لا يوجد اي شيء ■
س21: هل يوجد ميزانيه مخصصه سنويا لتحديث برامج الفيروسات وتراخيص انظمة الجدار الناري وشراء الاصدارات الحديثه من التطبيقات والبرامج التي تعتمد عليها الشركه؟	■ نعم يوجد ميزانيه مخصصه ومحدده لكل البنود الاساسيه للتحديث والتجديد ■ يوجد ميزانيه لبعض البرامج والاساسيات ■ يوجد ميزانيه ولكنها ضعيفه ■ لا توجد ميزانيه مخصص
□ س 23: ما هي الأدوات التي تستخدمها لزيادة الوعي داخل شركتك؟ورش عمل وندوات دوريه سنويا	■ استضافة متخصصين لزيادة التوعية ■ استخدام السوشيال ميديا (رسائل واتس اب دوريه - وموقع الشركة عبر فيسبوك) لنشر الوعي ■ توزيع منشورات او ايميلات بالمخاطر ■ يتم الاعتماد علي مهارات ووعي الموظف ■ لا يوجد اي انشطه لزيادة الوعي ■ منصات التعلم الإلكتروني(E-learning Platforms) ■ اخري
س25: كيف تقوم بتقييم/مراجعة نقاط الضعف لدى الشركة الخاصة بك؟	■ استعين بمقيم خارجي لفحص المنظومة بالكامل ■ يقوم فريق الشركة بفحص المنظومة بالكامل وتقديم تقارير بذلك ■ لا أقوم باي اعمال تقييم ■ موافق بشده

س27: أياً من الاختراقات التالية تعرضت لها الشركة؟	■ ايميلات خادعه ■ محاولة سرقة بيانات ■ التعرض لهجمات إيقاف الخدماتDDOS, DOS…etc ■ الإصابة بالفيروسات وبرامج الدودية وغيرها ■ محاولات تشفير البيانات والابتزازRransomware ■ انتحال الشخصيةSocial Engineering ■ اختراقات اخري ■ لم يحدث اي اختراقات
س28: ما الحدث الذي قد يدفعك للامتثال واتخاذ إجراءات وقائية صارمه لتطبيق سساسات الأمن السيبراني بفاعلية؟	■ وجود قانون ملزم للشركات او توجيهات من مرفق تنظيم الاتصالات ■ التعرض لخساره ماليه نتيجة الخروقات السيبرانيه ■ تعرض سمعة الشركه للخطر ■ تسريب بيانات هامه من الشركه وغير معلوم السبب ■ التعرض للابتزاز الالكتروني ■ تعرض شركات اخري معروفه لاختراقات سيبرانيه سببت خسائر فادحه ■ انا اعلم المخاطر جيدا واقم ببذل اقصي جهد ■ تعطل اعمال الشركه / موقع الشركه / خدمات الشركه ■ لتحقيق مستلزمات القبول في مناقصات عامه او طلب مباشر من الجهات التي اعمل معها ■ اذا زاد معدل الاختراقات التي اتعرض لها سنويا ■ انا اعلم المخاطر جيدا ولا يوجد سبب لاخذ إجراءات خاصه
س29: عند محاولة تأمين الشركة ضد الهجمات السيبرانية، أي من الأطر الدولية التالية سوف تقوم باتباعها؟	■ الايزوIS27001 ■ NIST ■ SOC 2 ■ Essecialy cybersecurity ■ لم اسمع بها ولا استخدمها