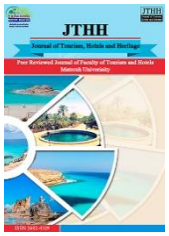


**Journal of Tourism, Hotels and Heritage (JTHH)**
**Journal Homepage:** https://sjs.journals.ekb.eg
**Print ISSN:** 2682-4329
**Online ISSN:** 2735-3044

# Organizational Culture and Its Role in Strengthening Cybersecurity Systems for Tourist Airport Employees in Egypt

# الثقافة التنظيمية ودورها في تعزيز نظم الأمن السيبراني لموظفي المطارات السياحية في مصر

تقوى محمد عيسوي*

**Article Info** **معلومات المقالة**

**Article Language:** Arabic **لغة المقالة:** العربية

**Vol. 9 No.1, (2024) pp. 95-116** | https://doi.org/10.21608/SIS.2024.305861.1175

**Abstract**

After the COVID-19 outbreak, the world has become more dependent on wireless communications and online payment systems, and the adoption of emerging technological solutions has accelerated dramatically. However, cybersecurity threats were actually available, which prompted most service organizations to prioritize in their budgets accurate system adoption to confront potential threats. Otherwise, employee awareness of those organizations of these systems may save a lot of time and reap huge profits from adopting new technology in the work environment. As such, the existing research seeks to highlight the impact of tourism airport employees' perceptions of cybersecurity system implementation on enhancing their perceived awareness of its effectiveness. The current research also examines the moderating role of the organizational culture of these employees in the perception and awareness stages of implementing cybersecurity systems in operational processes within tourist airports. A total of 266 responses were collected from tourist airport employees in Egypt: Marsa Alam, Luxor, Sharm El-Sheikh, and Hurghada. The data was analyzed using partial least squares-based structural equation modeling. The results proved that there is a positive and significant effect for each dimension of implementing cybersecurity systems: security enhancement, security privacy, and data confidentiality, on perceived awareness from an airport employee perspective. The results also indicated that organizational culture strengthened the positive nexus between perceived awareness and security enhancement, security privacy, and data confidentiality provided by cybersecurity systems. The research results concluded that improving organizational culture, enhancing training programs, developing clear cybersecurity policies, supporting various departments to effectively implement systems, and motivating employees to cooperate in protecting information are essential.

*Keywords:* Organizational culture; cybersecurity; tourism airports; employees; perceived awareness.

**الملخص**

دفعت التهديدات السيبرانية كافة المؤسسات إلى تخصيص ميزانيات ضخمة لتعزيز الإجراءات الإحترازية لتقليل المخاطر المحتملة الناتجة عنها، وإعتماد نظم أمن متطورة لمواجهة الهجمات الإلكترونية وخاصة المتعلقة بقطاع الطيران المدني في ظل التحول الرقمي الذي يشهده العالم الآن. في حين أن إدراك موظفي تلك المؤسسات لطبيعة وأهمية عمل هذه الأنظمة دور كبير في تحسين كفاءة العمل، وتعظيم الربحية مع تعزيز جدوى إستراتيجية إعتماد مثل هذه الأنظمة في بيئات العمل المختلفة. على هذا النحو، يهدف البحث لتسليط الضوء على تأثير إدراك موظفي المطارات لتنفيذ أنظمة الأمن السيبراني في تعزيز وعيهم المتصور تجاه فعالية تلك الأنظمة، وأيضاً اختبار مدى دور الثقافة التنظيمية لهؤلاء الموظفين بين مرحلتي الإدراك والوعي لتنفيذ أنظمة الأمن السيبراني في العمليات التشغيلية بالمطارات السياحية، وكذلك، تقديم بعض التوصيات لتحقيق أفضل الممارسات والاستراتيجيات لتعزيز الوعي بنظام الأمن السيبراني لدى موظفى المطارات في مصر. قد تم الحصول على ٢٦٦ استجابة جُمعت من موظفي المطارات السياحية في مصر: الغردقة، الأقصر، شرم الشيخ ومرسى علم. تم تحليل البيانات باستخدام نمذجة المعادلات البنائية القائمة على المربعات الجزئية الصغرى. أسفرت النتائج عن وجود تأثير إيجابي ومعنوي لكل من أبعاد تنفيذ أنظمة الأمن السيبراني: التعزيز الأمني، الخصوصية الأمنية وسرية البيانات في الوعي المتصور تجاه تنفيذ تلك الأنظمة من منظور موظفي المطارات. كما أشارت النتائج إلى أن الثقافة التنظيمية قد عززت العلاقة الإيجابية بين الوعي المتصور وكل من التعزيز الأمني، الخصوصية الأمنية وسرية البيانات التي توفرها أنظمة الأمن السيبراني. خلصت نتائج البحث إلى ضرورة تحسين الثقافة التنظيمية، تعزيز برامج التدريب، تطوير سياسات واضحة للأمن السيبراني، دعم الإدارات المختلفة لتنفيذ الأنظمة بفعالية، وتحفيز الموظفين على التعاون في حماية المعلومات.

*الكلمات الدالة:* الأمن السيبراني، الثقافة التنظيمية، المطارات السياحية، الموظفين، الوعي المتصور.

* مدرس، المعهد العالي للدراسات النوعية بالهرم

## المقدمة

أصبحت قضية أمن وحماية المعلومات من أهم قضايا العصر، حيث أصبح نجاح أي مؤسسة يعتمد بشكل كبير على مدى قدرتها على الحفاظ على سلامة وسرية ما تمتلكه من معلومات، ونظراً لهيمنة التحول الرقمي علي شتى أعمال القطاعات السياحية والفندقية، والطيران المدني في المطارات، واتصال العديد من تلك الأعمال والمعلومات والأنظمة والبني التحتية الخاصة بها بشبكات الأنترنت(Kim&Solomon, 2010; Rîndasu, 2017; Eilts, 2020; Abeyratne, 2020)، اصبحت هذه القطاعات اكثر عرضة للأخطار المتعلقة بالأختراقات المعلوماتية والهجمات السيبرانية بين الحين والآخر، وما يترتب عليها من تعطل وتوقف خدماتها وإرباك أنظمة التشغيل والبني التحتية الحيوية وقرصنة واستغلال البيانات، والتأثير بالسلب علي تدفق معلوماته (المري،٢٠٢٣). وقد أشار Berlilana et al. (2021) إلى الاستطلاعات السابقة التي أكدت على أن أكثر من ٩٠٪ من موظفي الإدارة الأمنية في مختلف المؤسسات الخدمية لم يكونوا مستعدين للتعامل مع هذه الهجمات. هذا النقص في الاستعداد أدى إلى تفاقم الوضع، مما يشكل تهديداً للأمن القومي وللبنى التحتية للقطاعات والخدمات الحيوية ذات الأولوية (Abeyratne, 2016; Eilts, 2020). علاوة على ذلك، تسببت الهجمات السيبرانية الموجهة ضد مقدمي خدمات الملاحة الجوية ومرافق الطيران الوطنية في خسائر مالية هائلة للدول قُدرت بتريليونات الدولارات. فقد تكبد قطاع الطيران المدني خسائر بلغت حوالى ٢٥٢ مليار دولار في عام ٢٠٢٠ (Usama et al., 2024). ومن المتوقع أن تصل هذه الخسائر إلى ما يقارب ٢٣ تريليون دولار بحلول عام ٢٠٢٧، مما يبرز تأثير الهجمات السيبرانية الكبير على هذا القطاع الحيوي، هذا بالإضافة إلى تجنب العديد من المؤسسات الإبلاغ عن حوادث الهجمات الإلكترونية التى تعرضت لها حمايةً سمعتها فى أذهان عملائها(Pearson, 2014). لذا، كان لزاماً وضع آليات لصد هذه الهجمات وتوفير ضمانات أمنية داخل هذه البيئة الرقمية لحماية أمن وسلامة المعلومات والشبكات والأنظمة الإلكترونية. يبرز في هذا السياق أهمية الأمن السيبراني، المعني بحماية البيانات والشبكات والأنظمة الإلكترونية من الهجمات والاختراقات.

في سياق قطاع الطيران، يمكن تصنيف الهجمات السيبرانية– سواء قام بها أفراد أو كيانات خاصة أو دول– التي تستهدف مرافق وشركات الطيران المدني إلى ثلاثة أنواع رئيسية (Nobles,2019)، النوع أو الجيل الأول يتضمن اختراق أنظمة البرمجيات وإدارة التحكم في المطارات وروابط الإتصالات واجهزة الإستشعار والرادارات، مما يمكن أن يسبب تعطيلًا مؤقتًا للرحلات أو التسبب في قيام أجهزة الاستشعار بالإبلاغ عن معلومات غير صحيحة، أو جعل الأجهزة والأنظمة غير متاحة من خلال هجمات رفض الخدمة(Kurt et al., 2018; Alansari et al., 2019; Klenka,2021) ،أما النوع أو الجيل الثاني، فيشير إلى هجمات أكثر تقدمًا لتشمل تقنيات أكثر تطورًا مثل البرمجيات الخبيثة التي تستهدف تغيير البيانات بشكل جزئي أو كلي، والبني التحتية لهذا القطاع بشكل أساسي(Jeyakodi, 2015)، أما الجيل الثالث فيتسم بتكامل التكنولوجيا والتأثير الواسع لإستهداف الأنظمة المتصلة بالإنترنت والحوسبات السحابية التي تستهدف تعطيل الخوادم وإغلاق الخدمات الرقمية للمطارات، واختراق البيانات الحساسة للمسافرين وأمتعتهم، بالإضافة إلي بيانات موظفي المطارات(Gallegos-Segovia et al.,2017; George & Thampi,2019) ، مما يعرض الملاحة الجوية لمخاطر متزايدة نتيجة تدهور الجودة الشاملة للخدمات المقدمة والتأثير بالسلب علي تجربة المسافرين (Suciu et al., 2018)، ومع كل ابتكار جديد في مجال تكنولوجيا المعلومات والاتصالات في هذه الصناعة، سيكون الجانب الآخر في انتظار اختبار نقاط الضعف، وربما شن هجمات سيبرانية معقدة نظراً لطبيعة هذه الصناعة الحساسة (Elmarady & Rahouma, 2021)

الجدير بالذكر، تعرض مطار القاهرة الدولي لهجوم سيبراني في نوفمبر ٢٠٢٣، والذي استهدف موقعه الإلكتروني بشكل مباشر دون التأثير على أنظمته الداخلية. أكدت وزارة الطيران المدني المصرية نجاحها في صد الاختراق بفاعلية، حيث تم حجب الموقع كإجراء احترازي حتى التأكد من استعادة جاهزيته، مع توفير خدمات بديلة غير متأثرة بالحادثة. تم تأمين جميع البيانات الحساسة المرتبطة

بالموقع، بما في ذلك بيانات المسافرين وشركات الطيران والأسواق الحرة والاستراحات بالمطار. أعلنت جماعة القرصنة "أنونيموس" مسؤوليتها عن الهجوم، الذي أدى إلى إغلاق تطبيق مطار القاهرة وتعطل موقعه الإلكتروني لمدة ٢٠ ساعة، بالإضافة إلى استهداف خدمة البريد الإلكتروني بالمطار. تأكدت السلطات المصرية أن الهجوم تم من خارج البلاد(وزارة الطيران المدني المصرية: المركز الإعلامي، ٢٠٢٣).

بناءً على ذلك، أصبح موضوع الامن السيبراني محور اهتمام العديد من الدراسات، وينبغي الذكر إن صناعة السياحة ليست بمنأى عن هذه المخاطر. لذلك، يعد تطوير أدوات أمنية فعالة لاكتشاف الهجمات والتخفيف منها أمراً بالغ الأهمية لحماية شبكات الإنترنت بالمطارات، بالإضافة إلى تنفيذ العديد من حلول الأمن السيبراني وتحديثها وإعادة معايرتها بسرعة لاكتشاف التهديدات السيبرانية الجديدة ومواجهتها بشكل فعال.

## الدراسات السابقة

استعرض Chiappetta & Cuozzo (2017) نقاط الضعف في الأمن السيبراني في البنية التحتية الحيوية للمنافذ والمطارات الذكية، ومناقشة السياسات الأمنية في أوروبا. بالتركيز على أنظمة SCADA، والتي تشمل وحدات القياس عن بعد، وقنوات الاتصال، وأجهزة الواجهة البشرية للمراقبة والتحكم. قدمت الدراسة نظام Hybrid Port، وهو حل أمني هجين يجمع بين أجهزة الاستشعار المادية والسيبرانية لتحسين عملية صنع القرار والكشف عن الأحداث الأمنية.

سلطت دراسة Suciu et al. (2018) الضوء على تأثير الأعمال الإرهابية والهجمات السيبرانية على تطوير تدابير الأمن السيبراني المتقدمة. مع التركيز على الهجوم الإرهابي الذي وقع في سبتمبر ٢٠١١ في الولايات المتحدة الأمريكية باعتباره المحرك الرئيسي للابتكار في مجال أمن المطارات والأمن السيبراني. وكشفت مراجعة الأدبيات الخاصة بهم عن نقاط الضعف في تطبيقات الأمن السيبراني الحالية في المطارات. وسلطت الدراسة الضوء على أنظمة المطارات الحيوية المعرضة للإختراق. مع تقديم بعض السيناريوهات للهجمات الإرهابية المتوقعة ضد البنية التحتية للمطارات، مع توضيح تأثيراتها. ومع ذلك، لوحظ أن الدراسة تفتقر إلى مناقشة مختلف أنواع الهجمات الإلكترونية.

استكشف Willemsen & Cadee(2018) أمن المطارات، مع التركيز على تكامل التدابير المادية والأمن السيبراني. تم القيام بتقسيم رحلة المسافرين في المطارات إلى مناطق ذات احتياجات أمنية متميزة. مع تسليط الضوء على نقاط الضعف في الأنظمة القديمة، وخاصة نظام مناولة الأمتعة، الذي غالبًا ما يفتقر إلى التحديثات التكنولوجية ويكون عرضة للهجمات الإلكترونية. وتم عرض التهديدات الرئيسية المعتمدة على الخدمات السحابية، وخدمات الطرف الثالث غير الآمنة. وأوصت الدراسة بتعزيز التعاون بين المطارات وأصحاب المصلحة لتحسين الأمن العام.

أجرى Lykou et al.(2018) بحثًا حول جاهزية المطارات للأمن السيبراني وقدرتها على مواجهة الهجمات السيبرانية. توصلت الدراسة إلى تفاوت مستويات تكامل تكنولوجيا إنترنت الأشياء، وتم تصنيف ٢٧٪ من المطارات الأمريكية والأوروبية على أنها "مطارات ذكية"، وتقسيم أفضل الممارسات الحالية للأمن السيبرانى إلى مجموعات فنية وتشغيلية وسياسات ومعايير. تم تحديد نقص الوعي الأمني ومشكلات الاتصال بالإنترنت على أنها أعلى مخاطر الأمن السيبراني. وقد ركزت الدراسة في المقام الأول على وجهات نظر موظفي تكنولوجيا المعلومات، بغض النظر عن توضيح تطبيقات محددة لإنترنت الأشياء وتكنولوجيا المعلومات ونقاط الضعف المرتبطة بها في الأمن السيبراني.

بحث Lekota & Coetzee(2019) في الاستعداد السيبراني لقطاع الطيران في منطقة جنوب الصحراء الكبرى، ومقارنته بالمعايير الدولية وتسليط الضوء على أوجه القصور في السياسات الحالية وأفضل الممارسات والأنظمة القديمة التي تعرض استقرار المطارات والطائرات للخطر. توصلت الدراسة إلى بعض النتائج منها أن الأمن السيبراني ليس له أولوية في جنوب أفريقيا ومنطقة جنوب الصحراء الكبرى، حيث لا توجد سلطة مركزية لتخطيط السياسات والاستعداد، ويظل التركيز على الأمن المادي. وشددت الدراسة على الحاجة إلى أطر لتعزيز الأمن السيبراني في المنطقة، مع ضرورة تصنيف أفضل الممارسات إلى التخطيط والاتصال والتحليل.

أجرى Aboti(2019) مراجعة شاملة لتطبيقات إنترنت الأشياء في قطاع الطيران التجاري، مع تسليط الضوء على النمو السريع لتكنولوجيا إنترنت الأشياء وتكاملها في مختلف إعدادات الطيران، مع تحديد المخاوف الأمنية الهامة المرتبطة بإنترنت الأشياء، بما في ذلك خصوصية البيانات، وتوافر الخدمة، وبيانات اعتماد الجهاز الافتراضي، ودور الذكاء الاصطناعي في تحليل البيانات. كما تم تناول الهجمات المحتملة التي يمكن أن تستغل نقاط الضعف في المطارات أو الطائرات الذكية. ومع ذلك، لم تتطرق الدراسة إلى تأثير هذه الهجمات على أمن المطارات والطائرات.

بحثت دراسة Suciu et al.(2019) في نقاط الضعف في الأمن السيبراني المتأصلة في المطارات الذكية، ودرست سبل الهجوم الجديدة الناتجة عن دمج التقنيات الذكية في أنظمة المطارات والطائرات. مع توضيح مدى تشكيل الأجهزة الشخصية للركاب لخطر التهديدات المحتملة للبنية التحتية الحيوية للمطارات. من خلال سيناريوهات حملات التصيد الاحتيالي وهجمات انتحال البيانات على مراكز عمليات المطار، وقد اقترح البحث تصنيف البيانات الواردة ووضع استراتيجيات للرد على هذه الهجمات وتخفيف حدتها.

استعرض Rajapaksha & Jayasuriya (2020) التطبيقات الذكية المستخدمة في العمليات الخاصة بمحطات الركاب والمسافرين في المطار والأنظمة الفرعية الأخرى. وقد أوجزت الدراسة الخاصة بهما مبادئ المطارات الذكية فضلاً عن تحليل تطبيقات إنترنت الأشياء الحالية. وتم تسليط الضوء على فوائد الاستجابة الأسرع للأزمات، وتحسين الفحص، وجمع البيانات، والاستخدام الأمثل للموارد. ومع ذلك، تناولت الدراسة أيضًا التحديات الخاصة بالأمن السيبراني فيما يتعلق بتطبيقات إنترنت الأشياء والتى من شأنها تؤدى إلى ظهور نقاط ضعف جديدة باستمرار. وشدد البحث على الحاجة إلى تحسين أساليب الكشف عن حوادث الأمن السيبراني والتخفيف من آثارها وأهمية تثقيف موظفي المطار. على الرغم من إدراج العديد من تطبيقات إنترنت الأشياء، إلا أن تحليل المراجعة لآليات الأمن السيبراني كان محدودًا.

درس Lehto(2020) تحديات الأمن السيبراني في قطاعات النقل البحري والطيران والسيارات، مع التركيز على التهديدات المستمرة المتقدمة (APTs) التي تستهدف البنية التحتية الحيوية. وشددت الدراسة على التطور المتزايد للهجمات السيبرانية وآثارها الخطيرة، لا سيما على قطاع الطيران. وسلطت الدراسة الضوء على نقاط الضعف التي أدخلتها أجهزة إنترنت الأشياء في المطارات والطائرات الذكية. مع الإشارة إلى الحاجة إلى إستحداث أنظمة شاملة لإدارة التهديدات والمخاطر ووضع معايير عالمية لتحسين المرونة السيبرانية. وحددت الدراسة فجوة في تقييم القدرات التقنية والبروتوكولات الأمنية للمطارات الذكية، مع التركيز على الحاجة إلى مزيد من البحث في أسطح الهجوم الجديدة وأساليب الاستغلال.

تناولت دراسة Koroniotis et al.(2020) مراجعة شاملة لتطبيقات المطارات الذكية الحالية والخدمات التي تدعم إنترنت الأشياء. كما أوضحت أيضًا أدوات الدفاع السيبراني المختلفة، بما في ذلك الذكاء الاصطناعي وتقنيات التنقيب عن البيانات، وقاموا بتحليل نقاط القوة والضعف فيها في سياق المطارات الذكية. علاوة على ذلك، صنفت الدراسة الأنظمة الفرعية للمطارات الذكية بناءً على غرضها وأهميتها، وأشارت إلى التهديدات السيبرانية التي يمكن أن تعرض أمن شبكات المطارات الذكية للخطر.

## الإطار النظري وتطوير الفروض

### مفهوم الأمن السيبراني

ظهر مصطلح " الأمن السيبراني" نظرياً لأول مرة في سبعينات القرن الحالي، ومع انتشار الشبكات الرقمية وتطور نظم الحوسبة تحول هذا المصطلح إلي مفهوم قابلاً للتطبيق، ليتم إطلاقه على كافة الإجراءات والممارسات المتعلقة بحماية أصول وأنظمة وتقنيات المعلومات الرقمية، وسلامة البيانات والبرمجيات المتصلة بالشبكات الإلكترونية الحاسوبية، ومنع الإختراقات الفيروسية للفضاء السيبراني بكافة تطبيقات الهواتف المحمولة والشبكات الإجتماعية فضلاً عن الخدمات المالية والتسوق عبر الأنترنت (السمحان، ٢٠٢٠)، ليصبح بذلك المجال الذي يتعلق بإجراءات ومقاييس ومعايير الحماية المفروض اتخاذها أو الالتزام بها، وذلك لمواجهة التهديدات والحد من آثارها في أسوأ الأحوال (الزهرانى، ٢٠٢٠). وبذلك يشمل الأمن السيبراني في المطارات اتخاذ التدابير اللازمة لحماية خصوصية وسرية فضاءها السيبراني من الهجمات السيبرانية، ويتضمن ذلك استخدام مجموعة من التقنيات المتقدمة والسياسات التنظيمية والإدارية لضمان استمرارية أنظمة البرامج والمعلومات الخاصة بالمطارات لمنع الوصول غير المشروع إلى المعلومات الإلكترونية ومنع استغلالها بطرق غير قانونية (السمحان، ٢٠٢٠).

### اسباب التهديدات السيبرانية الموجهة لقطاع الطيران المدني

علي الرغم من زيادة الإعتماد على الإتصالات اللاسلكية في الآونة الأخيرة، وأنظمة الدفع الإلكتروني خاصة مع تسارع استخدام تطبيقات ومفردات التكنولوجيا الناشئة بشكل كبير فى كافة القطاعات السياحية والفندقية والطيران المدني، وتفشي جائحة كرونا. إلا ان التهديدات السيبرانية الموجهة لصناعة الطيران تشكل مشكلة حقيقية، ويرجع تزايد التهديدات السيبرانية الموجهة لهذه الصناعة إلي عدة عوامل يمكن إجمالها في الآتى:

جاذبية قطاع الطيران المدني، حيث تعد صناعة الطيران احدي الصناعات الحيوية للإقتصادات الوطنية نظراً لدورها الكبير في التجارة والنقل والبنى التحتية (Iasiello, 2013). لذلك، فإنها تجذب اهتمام القراصنة بسبب البيانات الحساسة التي تتضمن أسماء المسافرين، وأرقام هوياتهم وجوازات سفرهم، ومعلوماتهم الشخصية كمحل الإقامة وصورهم وبصماتهم ووجهات سفرهم. مما يمكنهم من استخدام هذه البيانات لأغراض غير قانونية مثل سرقة بيانات بطاقات الائتمان أو الإحتيال باسمائهم وإبتزازهم أوابتزاز شركات الطيران ذاتها(Klenka, 2021; Kovacic et al.,2022) .

هذا بالإضافة إلى رقمنة قطاع الطيران علي مستوي العالم، فعلى الرغم من تعدد الاستفادة من التكنولوجيا المتقدمة في مجال الطيران المدنى، لمواكبة التطورات في إدارة حركة الملاحة الجوية وتحقيق أمان أكبر للرحلات (Lykou et al., 2020). إلا ان رقمنة الصناعة بطابعها الشبكي في ظل ربط أنظمة المعلومات الخاصة بالطائرات على مستوى العالم لتأمينها وتحديد مساراتها وتقليل مخاطر الحوادث، واعتماد تقنيات الجيل الخامس والذكاء الاصطناعي يسفران عن تحدياً ضخماً أمام قطاع الطيران المدني لمواجهة التهديدات السيبرانية المستهدفة له والتي تهدد بسرقة وقرصنة البيانات واختراق أنظمة التشغيل الحيوية (Choi et al., 2018).

فضلا عن إمكانية تعدد التهديدات السيبرانية الموجهة لصناعة الطيران، حيث تحولت الطائرات الطائرات في السنوات الأخيرة إلى ما يمكن وصفه بـ مراكز بيانات طائرة، حيث تتضمن هذه التحولات تعدد الأنظمة التي يتعين حمايتها وتأمينها ضد الهجمات السيبرانية، مثل أنظمة الاتصال والإقلاع، وأنظمة حجز التذاكر عبر الإنترنت والهواتف الذكية، وأنظمة الترفيه داخل الطائرة، وتتبع أمتعة المسافرين، وأنظمة الهبوط الآلي، إضافة إلى عناصر أخرى مثل سلاسل التوريد للإلكترونيات الطائرات وأنظمة التحكم لإنترنت الأشياء، وأنظمة التشغيل الآلي في المطارات، والتطبيقات الإلكترونية، ومنصات تجربة الطيران عبر الإنترنت والتجارة الإلكترونية.

مما يتطلب حماية شاملة لكافة أنظمة الاتصال والإقلاع وحجز التذاكر عبر الإنترنت، لذلك يجب تدريب الطواقم على التصدي للهجمات السيبرانية(Paraskevas, 2022).

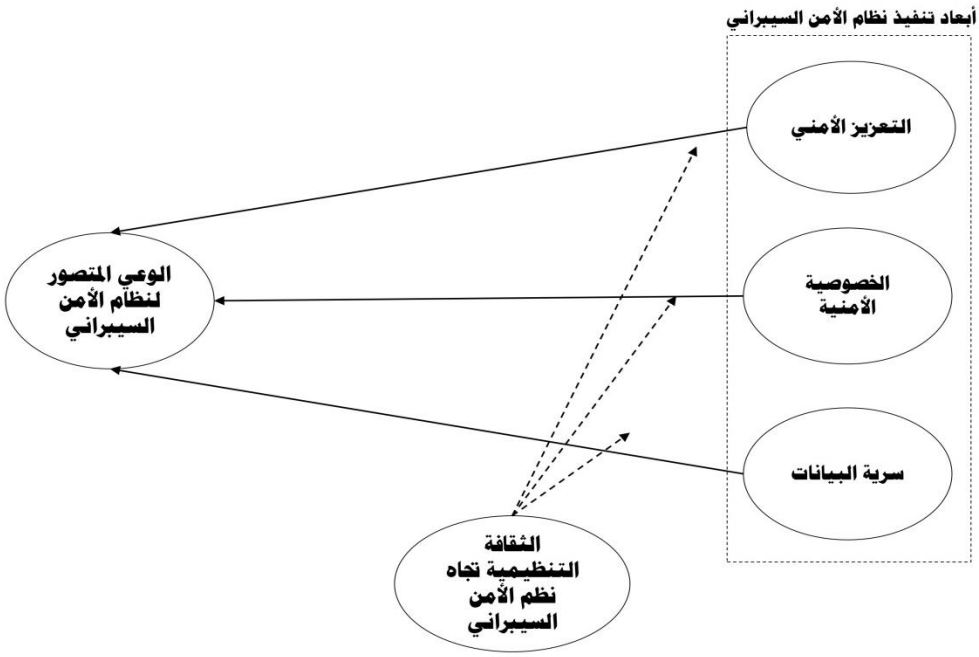
وأيضاً أهمية أمان مرفق الطيران للسمعة الدولية، حيث يعكس أمان الطيران قدرة الدول على حماية أمنها، وتأثير التراجع في الثقة الدولية يمكن أن يؤثر على صورتها العامة ومصداقيتها,Marcialr& Launer). (2019 لذا، يجب الامتثال لمعايير الأمان السيبراني وحماية خصوصية المستخدمين للحفاظ على السمعة الدولية وكذلك الإهتمام بتأهيل الكوادر البشرية وزيادة برامج التدريب الخاصة بالأمن السيبراني وأمن المعلومات ,Ahmed) (2021

وكذلك، التحديات الخاصة بالإفصاح عن الهجمات السيبرانية، حيث يترتب علي النقطة السابقة عدم تفضيل الدول للإفصاح عن تعرض مرافقها الحيوية للإختراقات مما يحد من الجهود الرامية إلى تحديد أسباب ودوافع ومصادر الهجمات(Albataineh&Alsmadi, 2019)، وبالتالي فإن التهديدات السيبرانية المختلفة تتطلب شفافية وتعاوناً دولياً أفضل في تبادل المعلومات، لتعزيز أمن ومرونة صناعة الطيران والمطارات، والتصدي للهجمات بشكل فعال ومسبق(Pearson, 2014).

في هذا الصدد، قامت شركة ميناء القاهرة الجوي بتطبيق حزمه جديده من البرامج والتطبيقات الإلكترونية المؤمنة بمختلف القطاعات، تحقيقاً لرؤية مصر ٢٠٣٠ المتعلقة بتعزيز الثقة في بنية الاتصالات والبنية التحتية للمعلومات، بغرض تحقيق الإدارة الإلكترونية المتكاملة بالشركة للربط بين جميع قطاعات المطار من خلال شبكه معلوماتية متكاملة موحدة وآمنة، وتفعيل تطبيقات حديثة تسهل عمليه الاتصال لتحقيق أعلى جودة من الخدمة المقدمة، كما تم دعم خطة المراقبة الأمنية لجميع الأنظمة التشغيلية بالمطار، وتطوير رخص حماية شبكة المعلومات والبريد الإلكتروني من الفيروسات وربطها ببرامج أخرى لرفع مستوى الحماية لكافة أنظمة الأمن السيبراني في مطار القاهرة الدولي. وقد اوضح(2022) .Abdel-Al et al بعض من الجهود المصرية، بهدف تحقيق بيئة رقمية آمنة وموثوقة. تشمل هذه الجهود إنشاء المركز المصري للإستجابة لطوارئ تكنولوجيا المعلومات(سيرت) منذ عام ٢٠٠٩، لمواجهة التهديدات الأمنية السيبرانية وتحليل الأدلة السيبرانية والبرمجيات الخبيثة فضلاً عن فحص الثغرات واختبار الاختراقات. كما تم تشكيل المجلس الأعلى للأمن السيبرانى فى عام ٢٠١٤ للتأكد من توفير التمويل اللازم لضمان تنفيذ منظومة الأمن السيبراني بشكل فعال، والإطر التشريعية المنظمة لهذا النظام. ثم إصدار الإستراتيجية الوطنية للأمن السيبراني (٢٠١٧-٢٠٢١).

**النموذج البحثي**

يشير النموذج البحثي ( شكل رقم ١) إلى طبيعة وخصائص تطبيق أنظمة الأمن السيبراني في بيئة المطارات السياحية التي قد تتأثر بمستويات التعزيز الأمني والخصوصية الأمنية والحفاظ علي سرية البيانات. وبالتالي، فمن الممكن أن تؤدي زيادة مستويات الوعي المتصور للمتعاملين مع الخدمات الإلكترونية في هذه المطارات إلى تعزيز الفهم والتفاعل بشكل أفضل معها، إلا أنه قد يكون من الضروري إعادة النظر في هذه العلاقة بشكل دقيق نظرًا لاحتمالية فقدان القيم والمبادئ التي يتبعها موظفو المطارات خلال تنفيذ تلك الأنظمة.




**شكل ١. نموذج البحث**

**التعزيز الأمني**

يشير التعزيز الأمني إلى اتخاذ جميع الإجراءات والتدابير اللازمة لزيادة مستوى الحماية والأمان في النظام السيبراني، بهدف حماية الأنظمة التقنية والخدمات الإلكترونية من التهديدات المحتملة(Gunduz & Das, 2020) . يشمل ذلك استخدام جدران الحماية، وبرامج مكافحة الفيروسات، وأنظمة الكشف عن الاختراقات، والتحديث المنتظم للبرمجيات لسد الثغرات الأمنية (Alladi et al., 2020; Aslan et al., 2023). هذا ويُعَدُّ التعزيز الأمني في المطارات شيئاً حتمياً لحماية الأنظمة التشغيلية والبنية التحتية لتكنولوجيا المعلومات من الهجمات السيبرانية التي قد تعطل العمليات أو تعرض البيانات الحساسة لخطر القرصنة (Lykou et al., 2018; Djenna et al., 2021). فضلاً عن مساهمته في زيادة الوعي بأهمية الحماية الإلكترونية بين الموظفين، وتعزيز تبنيهم لأفضل الممارسات الأمنية (Bulgurcu et al., 2010). وأضاف على وآخرون(٢٠٢٢) أنه يجب أن يتضمن تعزيز الأمن السيبراني تحقيق كل من الآتى: **إدارة الوصول والصلاحيات، للتأكد** من وجود قائمة جرد دقيقة لكافة الأصول المعلوماتية والتقنية في المطارات، مع ضمان إدارة هويات الدخول والصلاحيات بشكل صارم للحماية من الوصول غير المصرح به للمعلومات التي قد تؤثر علي حركة التشغيل في المطارات. هذا بالإضافة إلى تعزيز حماية البريد الإلكتروني وأمن الشبكات لجميع الموظفين بالمطار. ولابد من التأكيد على ضمان الإستخدام الفعال لتقنيات التشفير لحماية الأصول المعلوماتية الحساسة بالمطارات. وكذلك تنفيذ استراتيجيات إدارة النسخ الاحتياطي للبيانات والمعلومات للوقاية من الأضرار الناجمة عن الهجمات السيبرانية المحتملة. مع حتمية إجراء اختبارات الاختراق بانتظام لتقييم مدى فعالية نظم الأمن السيبراني في المطارات، ومراقبة وتحليل سجلات حوادث الأمن السيبراني بشكل مستمر للكشف المبكر عن أي تهديدات وثغرات أمنية جديدة في النظام الأمنى المتبع والاستجابة الفورية لها وتصحيحها(Djenna et al., 2021) . وأخيراً، تنفيذ إجراءات الأمن المادي المناسبة لمنع دخول اي شخص غير مصرح له للوصول لمكاتب الأنظمة التقنية وذلك لحماية الأصول المعلوماتية والتقنية من السرقة والتخريب.

**الخصوصية الأمنية**

الخصوصية الأمنية في سياق الأمن السيبراني في المطارات تشمل جميع الإجراءات التقنية والإدارية التي تهدف حماية الركاب من التشارك غير المرغوب فيه لمعلوماتهم، سواء كان ذلك من قبل الأفراد أو المؤسسات أو الحكومات، بالإضافة إلى منع أي تدخل غير مصرح به بالتجسس أو الاختراق لاستخدام أو سوء الاستغلال للمعلومات والبيانات الإلكترونية الموجودة على نظم الاتصالات والمعلومات الخاصة بشركات الطيران أورواد المطارات، بما يضمن تأمين وحماية وسرية وخصوصية البيانات الشخصية (السمحان،٢٠٢٠). بما يضمن حماية سرية وسلامة البيانات الشخصية للركاب والموظفين أثناء النقل والتخزين، من خلال تشفير البيانات وتطبيق السياسات الصارمة لإدارة الوصول إلى المعلومات، بمنح صلاحيات محدودة للوصول للبيانات بناءً على احتياجات ومتطلبات الوظيفة فقط، ووضع وتنفيذ اللوائح المتعلقة بحماية الخصوصية وفق المتطلبات القوانين والتشريعات المتعلقة بذلك الشأن وأخيراً، تدريب الموظفين بشكل منتظم على أفضل الممارسات الأمنية وأهمية الحفاظ على الخصوصية والأمان السيبراني (Pierides, 2015; Lykou et al., 2018). قد أشار كل من Beecroft (2019) و(٢٠١٢) .Liu et al إلى الدور الحيوي الذي تمثله الخصوصية الأمنية في بناء الثقة لدى المستخدمين، سواء كانوا من ركاب أو موظفي المطارات، ومدى مساهمتها في تقليل المخاطر المحتملة المرتبطة بتسريبات البيانات والانتهاكات الأمنية.

**سرية البيانات**

تُعنى السرية في الأمن السيبراني باقتصار إمكانية الوصول إلى المعلومات والبيانات والملفات التقنية بشكل محدود على الأشخاص المعنيين فقط والمصرح لهم بذلك(Czuryk, 2022). لمنع أي تجاوزات أو ثغرات أمنية تقنية تلحق الضرر بها، مع التاكد من عدم إطلاع الأفراد غير المصرح لهم على هذه المعلومات، ويتم تحقيق ذلك من خلال استخدام تقنيات التشفير والتحكم في وإدارة الوصول بشكل دقيق وتطبيق سياسات أمنية صارمة(Corallo et al., 2021; Shukla et al., 2022). تكمن أهمية سرية البيانات في المطارات، فى عدة نقاط منها: حماية المعلومات المتعلقة بالرحلات ، والأمن، والركاب (Alabsi & Gill, 2021). الحفاظ على سرية البيانات يعزز الوعي بأهمية الحماية المعلوماتية كما يحد من احتمالية تعرض البيانات لخطر الاختراق أو الاستغلال غير المشروع، مما يسهم في تعزيز الأمان والثقة في النظم والخدمات الإلكترونية المستخدمة في المطارات (Aloul, 2012).

**الوعي المتصور بنظام الأمن السيبراني**

يعبر الوعي المتصور بنظم الأمن السيبراني عن مدى إدراك وفهم الموظفين والمستخدمين لأهمية النظم الأمنية والتدابير المتبعة لحماية البيانات والمعلومات(Daud et al., 2018; Li et al., 2019) . بما يتضمن التعرف على المخاطر المحتملة، واتباع السلوكيات السليمة لمواجهة الهجمات المحتملة، مع اللإمتثال للسياسات والإجراءات الأمنية التقنية (Kharlamov & Pogrebna, 2021; Wong et al., 2022). مع العلم بأن زيادة الوعي المتصور يسهم في تحسين السلوك الأمني التقني بشكل كبير، وتعزيز قدرة المؤسسات على التصدي للتهديدات السيبرانية بشكل فعال(Trim & Lee,2019; George, 2023).

**الثقافة التنظيمية لنظام الأمن السيبراني**

تتعلق الثقافة التنظيمية لنظام الأمن السيبراني بالقيم والممارسات والسلوكيات التي تتبناها المؤسسة لتعزيز الأمن التقني بها (Georgiadou et al., 2022). تشمل هذه الثقافة التزام الإدارة العليا بالأمن السيبراني، وتوفير التدريب المستمر للموظفين، وتشجيع التواصل المفتوح حول التهديدات والممارسات الأمنية(Hasan et al., 2021; Hasani et al., 2023). هذا وتعتبر الثقافة التنظيمية القوية عاملًا حاسمًا في تعزيز الوعي الأمني والالتزام بالتدابير الأمنية المعلوماتية، مما يساهم في بناء بيئة عمل آمنة ومحمية من الهجمات السيبرانية(Aksoy, 2024). وقد أوضح البيشي (٢٠٢١) الآثار السلبية المترتبة على الإنتهاكات والإختراقات الخاصة بالأنظمة السيبرانية، المتمثلة في فقدان ثقة الجمهور المستهدف، وانتشار الكلمة المنطوقة السلبية وتعظيم الشعور بعدم رضاء

العملاء، وتدهور السمعة والضرر بالعلامة التجارية للمؤسسة، والنتائج السلبية الأخرى مثل إنخفاض هامش الربح في المستقبل القريب والبعيد(Abd El-Maksoud, 2024) .

وقد أشار حمود (2023) إلى إمكانية إستغلال المؤسسات قدرتها علي تمتعها بأنظمة أمن سيبراني صعبة الإختراق، واعتمادها تدابير الامتثال الأمني المتقدمة التي تتوافق مع المعايير واللوائح السارية لخلق فرصًا فريدة لتعزيز ثقافتها التنظيمية وإظهار ريادتها مجال أمن المعلومات. يمكن للمطارات بناء ثقافة داخلية وهوية وصورة ذهنية خارجية حول الأهمية التى توليها لخصوصية عملائها وأمنهم ، مما يؤكد التزامها الجاد بالأمن وتعزيز الثقة في الخدمات التي تقدمها. ولذلك يتضح أهمية تدريب الموظفين، الذين يمثلون النواة الأولى للوصول إلى الأنظمة والبرامج التقنية قبل المتسللين والمخترقين الإلكترونيين، حيث يساهم هذا التدريب في زيادة معرفتهم ووعيهم حول الهجمات السيبرانية ويعزز استجاباتهم تجاه مثل هذه التحديات(Chen&Fiscus, 2018) .

## الدراسة الميدانية

### منهج وتصميم البحث

تهدف الدراسة الميدانية إلى التحقق من مدى دور إدراك موظفي المطارات السياحية لتنفيذ أنظمة الأمن السيبراني بالوعي المتصور نحو تنفيذ تلك الأنظمة بمصر، حيث تُعتبر مصر من بين الوجهات السياحية الأكثر أمانًا لتقديم خدماتها السياحية المختلفة. وذلك بالإعتماد على استخدام التصميم الكمي القائم على المنهج الوصفي التحليلي باستخدام الاستبيانات الورقية؛ كما تم اختيار المطارات السياحية (الغردقة، الأقصر، شرم الشيخ ومرسى علم)؛ ليكونوا وحدة التحليل في هذه الدراسة، وذلك نظرًا لكونهم الأكثر استقبالًا للوافدين أو المسافرين بشكلٍ ملحوظٍ على مدار العام بأغراض سياحية (وزارة الطيران المدنى: الشركة المصرية القابضة للمطارات والملاحة الجوية، ٢٠٢٣).

تم تقسيم الاستبيان لثلاثة محاور رئيسية. المحور الأول (مدى تنفيذ نظام الأمن السيبراني)، والتي تم قياسه بالاعتماد على ثلاثة متغيرات فرعية، وذلك بالإستعانة بحمود (٢٠٢٣): سرية البيانات بخمس عبارات، الخصوصية الأمنية بست عبارات، والتعزيز الأمني بخمس عبارات. أما المحور الثاني (الوعي المتصور بنظام الأمن السيبراني)، فقد تم قياسه بخمس عبارات، من خلال الإستعانة بمقياس Tejay and Mohammad (2023). وفي النهاية المحور الثالث (الثقافة التنظيمية تجاه نظام الأمن السيبراني)، والتي تم اعتماد ست عبارات تم تكيفها من Tejay and Mohammad (2023). وقد تم تصميم الإستمارة طبقاً لمقياس ليكرت السباعي التي يتراوح ما بين ١ = لا أوافق بشدة و٧ = أوافق بشدة.

على هذا النحو، يمكن إفتراض أن إدراك موظفي المطارات السياحية لأبعاد تنفيذ الأمن السيبراني سيزيد من وعيهم تجاه الأنظمة القائمة على هذه التقنية الذكية، وذلك في حالة وجود مستويات مرتفعة أو منخفضة من الثقافة المتبعة بتلك المطارات، والتي تتمثل فيما يلي:

H1. يؤثر التعزيز الأمني لنظام الأمن السيبراني إيجابيًا في الوعي المتصور بنظام الأمن السيبراني.

H2. تؤثر الخصوصية الأمنية لنظام الأمن السيبراني إيجابيًا في الوعي المتصور بنظام الأمن السيبراني.

H3. تؤثر سرية البيانات لنظام الأمن السيبراني إيجابيًا في الوعي المتصور بنظام الأمن السيبراني.

H4. تقوي الثقافة التنظيمية العلاقة بين التعزيز الأمني والوعي المتصور بنظام الأمن السيبراني.

H5. تقوي الثقافة التنظيمية العلاقة بين الخصوصية الأمنية والوعي المتصور بنظام الأمن السيبراني.

H6. تقوي الثقافة التنظيمية العلاقة بين سرية البيانات والوعي المتصور بنظام الأمن السيبراني.

### مجتمع وعينة البحث

تم اختيار موظفي المطارات السياحية المصرية ذات الصلة بالتعامل مع الأنظمة الإلكترونية كمجتمع بحثي. نظرًا لعدم توافر إحصائيات وتقديرات معلنة حول عدد موظفي المطارات السياحية في مصر، تم توظيف اقتراح Hair et al. (2019)، بأن حجم العينة المناسب لمجتمع غير معلوم، يجب أن يتجاوز ٢٠٠ مفردة. نتيجة لذلك، تم استخدام نهج العينات العشوائية المنتظمة للحصول على البيانات من المستجيبين بأربعة مطارات سياحية: مطار مرسى علم الدولي، مطار الأقصر الدولي، مطار شرم الشيخ الدولي ومطار الغردقة الدولي. تم تحديد ٣٦٠ مفردة كحجم عينة افتراضي في هذا البحث، أي بحوالي ٩٠ استجابة من موظفي كل مطار سياحي. بناءً على ذلك، تم التواصل مع أربعة من مسئولي العلاقات العامة في المطارات الأربعة للمساعدة في جمع البيانات من المستجيبين. في الفترة من يناير حتى مارس ٢٠٢٤، تم الحصول على ٢٧٣ استجابة مكتملة، بمعدل استجابة قدر بـ ٧٥.٨٪. بعد فرز الاستجابات باستخدام SPSS v.26، أسفرت النتائج أن هناك سبع استجابات تستوجب استبعادها من ملف البيانات النهائي؛ كونها تحتوي على قيم متطرفة تجاوزت في مجملها ١٥٪ عن الحدود المسموح بها للقيم الشاذة والمتطرفة في البيانات المجمعة. على هذا النحو، كان حجم العينة النهائي القابل للتحليل الإحصائي هو ٢٦٦، والذي يتخطى حجم العينة الافتراضي الموصى به من قبل Hair et al. (2019).

### أساليب تحليل البيانات

تم استخراج الإحصائيات الوصفية لشرح توزيعات الاستجابة باستخدام SPSS v.26 (جدول ١). بعد ذلك، تم تحليل البيانات باستخدام نمذجة المعادلات الهيكلية للمربعات الجزئية الصغرى لتقدير الفرضيات واختبار صحتها (Guenther et al., 2023). تتطلب هذه النمذجة حجم عينة صغير، ولا تفترض أن مجموعات البيانات يجب توزيعها بشكلٍ طبيعيٍ (Hair et al., 2017). بدلا من ذلك، اكتشف Sarstedt et al. (2022) أنه يمكن استخدام هذه النمذجة مع أحجام العينات التي تتجاوز ٥٠٠٠ مفردة. كما يعتبر سبب اختيار هذه النمذجة هو التعقيد الموجود في النموذج البحثي لوجود الدور المُعدل للثقافة التنظيمية، إلى جانب الطبيعة الاستكشافية للبحث الحالي (Hair et al., 2019). كما استخدم علماء السياحة هذه النمذجة على نطاق واسع بسبب قوتها الإحصائية، وقدراتها على تقييم الارتباطات الكامنة أثناء تقدير النموذج المقترح (Sarstedt et al., 2020). لذلك، تم استخدام هذه النمذجة لتقييم اثنين من النماذج الإحصائية: أولًا (نموذج القياس من خلال الصدق التقاربي والصدق التمييزي) وثانيًا (النموذج الهيكلي من خلال تقييم مدى ملائمة جودة النموذج، اختبار الفروض المباشرة والتحقق من فاعلية الدور المُعدل).

## النتائج والمناقشة

### الخصائص الديموغرافية للمستجيبين

**جدول ١. الخصائص الديموغرافية لموظفي المطارات (N = 266)**

| الخصائص | الفئة | النسبة | التكرارات | الخصائص | الفئة | النسبة | التكرارات |
|---|---|---|---|---|---|---|---|
| النوع | ذكر | 80.5 | 214 | الخبرة الوظيفية (السنوات) | أقل من ٣ | 61.3 | 163 |
| | أنثى | 19.5 | 52 | | ٣-٦ | 23.7 | 63 |
| المستوى التعليمي | ماجستير/دكتوراه | 30.1 | 80 | | أكثر من ٦ | 15 | 40 |
| | بكالوريوس | 37.2 | 99 | الفئة العمرية (السنوات) | أقل من ٣٠ | 49.2 | 131 |
| | ثانوي عام | 24.4 | 65 | | ٣٠-٤٥ | 8.3 | 22 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | دبلوم | 8.3 | 22 | | أكثر من ٤٥ | 42.5 | 113 |

يتضح من الجدول ١ أن جميع المتغيرات التي في ضوئها جمعت بيانات الدراسة قد تم تمثيلها، بمختلف الفئات. وقد كان ٨٠.٥٪ من الذكور بنسبة ٣٧.٢٪ من اجمالى درجة البكالوريوس. علاوة على ذلك، تميل الخبرات الوظيفية إلى نسبة ٦١.٣٪ من إجمالي المستجيبين ممن لديهم أقل من ثلاث سنوات. كما كشفت النتائج أن ٤٩.٢٪ من المستجيبين لديهم أعمار أقل من ٣٠ عام، يليهم ٤٢.٥٪ من المستجيبين الذين تزداد أعمارهم عن ٤٥ عام.

**تقييم نموذج القياس**

تم تقييم نموذج القياس باستخدام ثلاثة مؤشرات من الصدق التقاربي: ١) تشبع العبارات (أكبر من ٠.٧٠٨)، ٢) الموثوقية المركبة (أكبر من ٠.٧٠) و٣) متوسط التباين المستخرج (أكبر من ٠.٥٠) (Hair et al., 2019). أشارت نتائج جدول ٢ أن جميع قيم تشبع العبارات تجاوزت ٠.٧٠٨، مما يثبت أن النموذج يتمتع بصدق اتساق داخلي كافٍ. كما أسفرت النتائج الخاصة بذلك الجدول عن تخطي قيم الموثوقية المركبة قيمة ٠.٧٠، بما يثبت أن النموذج يتمتع بموثوقية عالية لجميع المتغيرات المقاسة. علاوة على ذلك، أثبتت النتائج الواردة بجدول ٢ أن قيم متوسط التباين المستخرج تجاوزت قيمة ٠.٥٠، بما يدل على أن هناك تباين ملحوظ بين عبارات كل متغير. بناءً على ذلك، أكدت جميع الدلائل السالف ذكرها على أن النموذج يتمتع بصدق تقاربي قوي (Sarstedt et al., 2020).

**جدول ٢. نتائج نموذج القياس**

| المتغيرات | كود العبارة | العبارات | تشبُع العبارات | الموثوقية المركبة | متوسط التباين المُستخرج |
|---|---|---|---|---|---|
| التعزيز الأمني | تعزيز ١ | تعتمد إدارة المطار وسائل فعالة لتحديد الموظفين الذين لديهم صلاحية الوصول لمواقع تخزين البيانات الحساسة. | 0.803 | 0.912 | 0.677 |
| | تعزيز ٢ | تستخدم إدارة المطار برامج مكافحة الفيروسات المرخصة بشكل دوري في الأجهزة المرتبطة بالتحكم في حركة الصعود والهبوط للطائرات. | 0.875 | | |
| | تعزيز ٣ | هناك آليات تخزين آمنة للوثائق ونسخ احتياطية للملفات في سحابة خاصة بإدارة المطار. | 0.787 | | |
| | تعزيز ٤ | لدى إدارة المطار وسائل فعالة لمراقبة البيانات وتحديد المخترق منها ثم عزلها ومحاولة علاجها. | 0.772 | | |
| | تعزيز ٥ | تُحدث إدارة المطار باستمرار آليات تعزيز حماية شبكاتها من خلال مواكبة الاتجاهات والمعايير العالمية المتخصصة بهذا المجال. | 0.870 | | |
| الخصوصية الأمنية | خصوصية١ | تقوم إدارة المطار بمراجعة صلاحيات مستخدمي الأنظمة الإلكترونية على فترات دورية منتظمة. | 0.813 | 0.942 | 0.730 |

| | | | | | |
|---|---|---|---|---|---|
| | خصوصية٢ | أواجه اختراقات متكررة على بريدي الإلكتروني التابع لهذا المطار. | 0.888 | | |
| | خصوصية٣ | تعتمد إدارة المطار تقنية المصادقة والتشفير لحماية الأنظمة والبيانات الحساسة من الهجمات السيبرانية. | 0.856 | | |
| | خصوصية٤ | يتم تشغيل وتحديث جدار الحماية باستمرار لمنع المتسللين من الوصول لبيانات المطار. | 0.869 | | |
| | خصوصية٥ | تتبنى إدارة هذا المطار سياسات الأمن السيبراني بمعايير عالمية للحد من حالات التجسس الرقمي. | 0.864 | | |
| | خصوصية٦ | تُقدم إدارة المطار ورش دورات تدريبية متخصصة لمستخدمي النظام الأمني لكيفية حماية البيانات. | 0.836 | | |
| سرية البيانات | سرية١ | لدي كلمة مرور قوية في هذا المطار تتكون من رموز وأحرف وأرقام صغيرة ومتوسطة. | 0.805 | 0.901 | 0.646 |
| | سرية٢ | يتم تبادل أرقام المرور السرية للأنظمة الإلكترونية بين موظفي هذا المطار. | 0.838 | | |
| | سرية٣ | تفرض إدار المطار على موظفيها تبديل كلمات المرور بشكل دوري. | 0.815 | | |
| | سرية٤ | توجد تعليمات إدارية صريحة حول حماية النظام الأمني من أي تلاعب في البيانات بهذا المطار. | 0.831 | | |
| | سرية٥ | يمتلك موظفو المطار معرفة كافية بتفاصيل عقوبات نشر الوثائق والمعلومات السرية. | 0.723 | | |
| الوعي المتصور بنظام الأمن السيبراني | وعي١ | أفهم المتطلبات والاحتياجات الأساسية لأمن نظم المعلومات في هذا المطار. | 0.817 | 0.924 | 0.708 |
| | وعي٢ | لقد قرأت وفهمت السياسة الأمنية لهذا المطار. | 0.872 | | |
| | وعي٣ | أتلقى بانتظام اتصالات مكثفة من هذا المطار بشأن الحوادث الأمنية وتنفيذ الضوابط الأمنية المناسبة. | 0.812 | | |
| | وعي٤ | أتلقى بانتظام اتصالات حول دوري ومسؤولياتي لتحقيق أهداف النظام الأمني في هذا المطار. | 0.836 | | |
| | وعي٥ | لقد حضرت ورشة عمل تدريبية حول كيفية الحفاظ على أمن البيانات في هذا المطار. | 0.868 | | |
| الثقافة التنظيمية | ثقافة١ | لقد خلقت إدارة المطار الوعي حول أهمية الالتزام بسياسات أمن نظم المعلومات. | 0.812 | 0.929 | 0.626 |

| | | | | | |
|---|---|---|---|---|---|
| تجاه نظام الأمن السيبراني | ثقافة٢ | تعزز إدارة المطار أهمية اتباع إجراءات أمن نظم المعلومات. | 0.793 | | |
| | ثقافة٣ | تعزز إدارة المطار أهمية مراقبة ضوابط أمن نظم البيانات الحساسة. | 0.811 | | |
| | ثقافة٤ | لقد خلقت إدارة المطار الوعي حول دور كل موظف ومسؤولياته فيما يتعلق بتحقيق أهداف أمن نظم المعلومات. | 0.778 | | |
| | ثقافة٥ | تقوم إدارة المطار بتوصيل أهمية الحفاظ على أمان البيانات لجميع موظفيها. | 0.762 | | |
| | ثقافة٦ | تعزز إدارة المطار أهمية الحفاظ على سرية المعلومات المتاحة. | 0.789 | | |

من ناحية أخرى، لتقييم الصدق التمييزي أحد مؤشرات تقييم نموذج القياس، تم الاعتماد على نسبة الارتباطات بين المتغيرات الكامنة Heterotrait-Monotrait، والتي يجب ألا تتخطى مؤشراتها الارتباطية عن ٠.٨٥ (Sarstedt et al., 2020). أسفرت نتائج جدول ٣ أن نسبة الارتباطات بين المتغيرات انحصرت بين ٠.٣١٦ و٠.٥٦٠، مما يؤكد عدم تخطي نسبة ارتباط أي متغير بمتغير آخر بأكبر من القيمة المسموح بها، بما يدعم تمتع نموذج القياس بصدق تمييزي كافٍ (Sarstedt et al., 2022).

**جدول 3. نتائج الصدق التمييزي**

| المتغيرات | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| ١. التعزيز الأمني | | | | | |
| ٢. الخصوصية الأمنية | 0.555 | | | | |
| ٣. سرية البيانات | 0.548 | 0.560 | | | |
| ٤. الوعي المتصور بنظام الأمن السيبراني | 0.481 | 0.495 | 0.422 | | |
| ٥. الثقافة التنظيمية تجاه نظام الأمن السيبراني | 0.316 | 0.379 | 0.372 | 0.462 | |

## تقييم النموذج الهيكلي

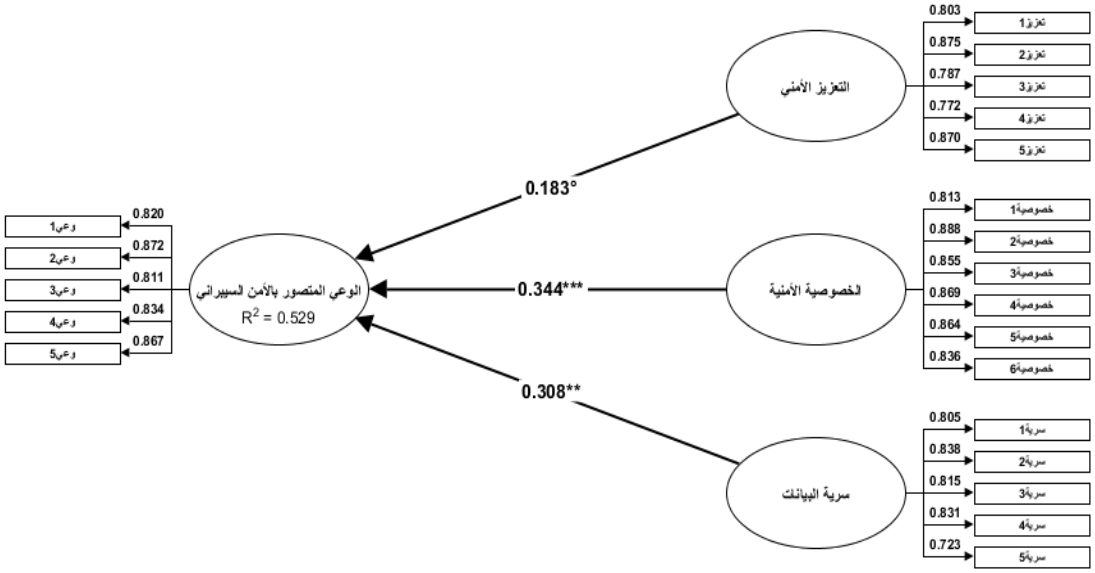
لتقييم النموذج الداخلي المقترح، تم إثبات صحة نموذج القياس باعتباره النموذج الخارجي (Hair et al., 2019). تم استخدام قيمة معامل التحديد التي يجب أن تتخطى ١٠٪ في التأثير المجمع للمتغيرات المستقلة في المتغير التابع، وحجم التأثير الذي يجب أن يتخطى ٠.٠٢ بين كل مسار ومسار آخر. أثبتت نتائج جدول ٤ وشكل أن قيمة معامل التحديد فسرت ٥٢.٩٪ من التباين في الوعي المتصور بنظام الأمن السيبراني، مما يثبت القوة التفسيرية لأبعاد تنفيذ أنظمة الأمن السيبراني من منظور موظفي المطارات السياحية (Sarstedt et al., 2020). كما كشفت قيم أحجام التأثير الواردة بجدول ٤ أن هناك تأثير ضئيل للتعزيز الأمني، وتأثير متوسط لسرية البيانات، بينما تأثير قوي للخصوصية الأمنية في الوعي المتصور بنظام الأمن السيبراني.

علاوة على ذلك، أشارت نتائج اختبار الفروض المباشرة (جدول ٤ وشكل ٢)، أن التعزيز الأمني لم يؤثر معنويًا في الوعي المتصور بنظام الأمن السيبراني ($\beta = 0.183$; $t = 1.933$; $p > 0.05$)، بما يؤكد على رفض الفرض الأول H1. على غرار ذلك، بينت

نتائج جدول ٤ وشكل ٢ أن الوعي المتصور بنظام الأمن السيبراني تأثر إيجابيًا ومعنويًا بالخصوصية الأمنية ( $\beta = 0.344$; $t = 5.029$; $p < 0.001$) وسرية البيانات ($\beta = 0.308$; $t = 3.091$; $p < 0.01$)، بما يدعم صحة الفرضين الثاني والثالث H2 and H3.

**جدول ٤. نتائج اختبار الفروض المباشرة**

| | المسارات | قيمة بيتا B | قيمة ت T-value | المعنوية P-value | حجم التأثير $f^2$ | معامل التحديد | النتيجة Result |
|---|---|---|---|---|---|---|---|
| H1 | التعزيز الأمني ← الوعي المتصور بنظام الأمن السيبراني | 0.183 | 1.933 | 0.053 | 0.030 | 0.529 | رفض الفرض |
| H2 | الخصوصية الأمنية ← الوعي المتصور بنظام الأمن السيبراني | 0.344*** | 5.029 | 0.000 | 0.149 | | قبول الفرض |
| H3 | سرية البيانات ← الوعي المتصور بنظام الأمن السيبراني | 0.308** | 3.091 | 0.002 | 0.085 | | قبول الفرض |




**شكل ٢. نتائج اختبار الفروض المباشرة**

تأسيسًا على ذلك، تم استخدام نهج اختبار التأثير المعدل ذو المرحلتين (Memon et al., 2021) لدراسة الثقافة التنظيمية نحو تنفيذ أنظمة الأمن السيبراني كمتغير مُعدل للعلاقة بين الوعي المتصور وأبعاد التنفيذ الفعلي. كشفت نتائج المرحلة الأولى بجدول ٥ أن الثقافة التنظيمية تجاه تنفيذ أنظمة الأمن السيبراني أثرت إيجابيًا ومعنويًا في الوعي المتصور بنظام الأمن السيبراني ( $\beta = 0.322$; $t = 6.232$; $p < 0.001$)، في حين كشفت نتائج المرحلة الثانية أن التعزيز الأمني لم يؤثر معنويًا في الوعي المتصور بنظام الأمن السيبراني ($\beta = 0.102$; $t = 1.828$; $p > 0.05$)، بينما تأثر الوعي المتصور إيجابيًا ومعنويًا بالخصوصية الأمنية ($\beta = 0.369$; $t = 7.312$; $p < 0.001$) وسرية البيانات ($\beta = 0.325$; $t = 5.206$; $p < 0.001$).

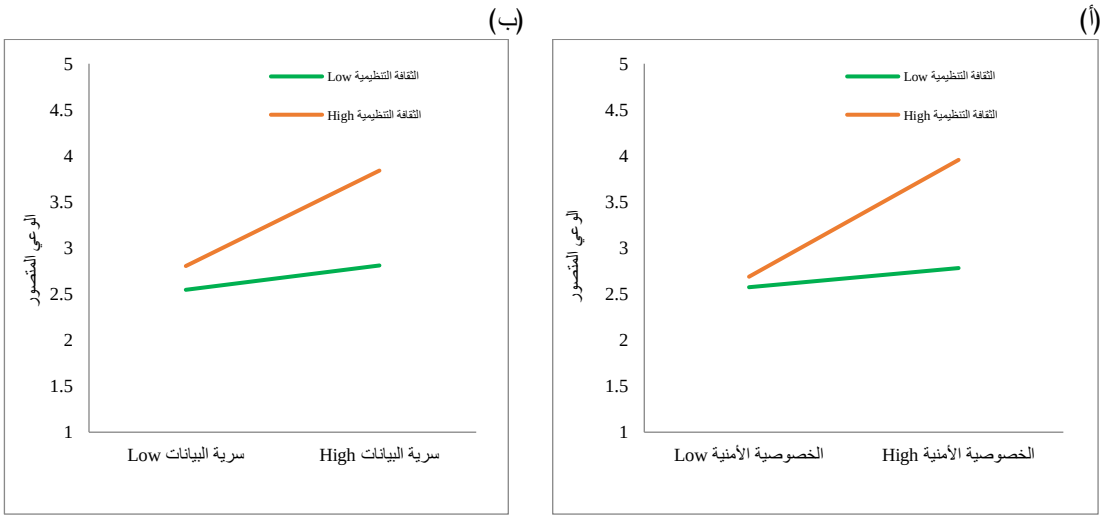
بالإضافة إلى ذلك، فإن مصطلح التفاعل للثقافة التنظيمية × التعزيز الأمني لم يكن معنويًا في الوعي المتصور بنظام الأمن السيبراني ($\beta = 0.083$; $t = 0.983$; $p > 0.05$)، مما يثبت رفض الفرض الرابع H4. على نقيض ذلك، أسفرت نتائج جدول ٥ أن مصطلح التفاعل للثقافة التنظيمية × الخصوصية الأمنية أثر إيجابيًا ومعنويًا في الوعي المتصور بنظام الأمن السيبراني ( $\beta = 0.265$; $t$

= 4.337; p < 0.01)، بما يدعم صحة الفرض الخامس H5. كما بينت نتائج جدول ٥ أن مصطلح التفاعل للثقافة التنظيمية × سرية البيانات أثر إيجابيًا ومعنويًا في الوعي المتصور بنظام الأمن السيبراني (β = 0.193; t = 3.654; p < 0.05)، بما يدعم صحة الفرض السادس H6.

**جدول ٥. نتائج تحليل الاعتدال لجاهزية البنية التحتية**

| | المسارات | قيمة بيتا B | قيمة ت T-value | المعنوية P-value | النتيجة Result |
|---|---|---|---|---|---|
| المرحلة الأولى | الثقافة التنظيمية تجاه نظام الأمن السيبراني ← الوعي المتصور بنظام الأمن السيبراني | 0.322*** | 6.232 | 0.000 | |
| المرحلة الثانية | التعزيز الأمني ← الوعي المتصور بنظام الأمن السيبراني | 0.102 | 1.828 | 0.073 | |
| | الخصوصية الأمنية ← الوعي المتصور بنظام الأمن السيبراني | 0.369*** | 7.312 | 0.000 | |
| | سرية البيانات ← الوعي المتصور بنظام الأمن السيبراني | 0.325*** | 5.206 | 0.000 | |
| H4 | التعزيز الأمني x الثقافة التنظيمية تجاه نظام الأمن السيبراني ← الوعي المتصور بنظام الأمن السيبراني | 0.083 | 0.983 | 0.082 | رفض الفرض |
| H5 | الخصوصية الأمنية x الثقافة التنظيمية تجاه نظام الأمن السيبراني ← الوعي المتصور بنظام الأمن السيبراني | 0.265** | 4.337 | 0.005 | قبول الفرض |
| H6 | سرية البيانات x الثقافة التنظيمية تجاه نظام الأمن السيبراني ← الوعي المتصور بنظام الأمن السيبراني | 0.193* | 3.654 | 0.028 | قبول الفرض |

لتأكيد التأثير المُعدل للثقافة التنظيمية، تم استخدام منحدرات التفاعل ذات المستوى المنخفض والمرتفع، كما هو مبين في شكل ٣ (أ وب). أشارت نتائج منحدرات التفاعل إلى أن التأثير الإيجابي للخصوصية الأمنية وسرية البيانات في الوعي المتصور كان أقوى عندما كان لدى موظفي المطارات السياحية لديهم مستويات عالية من الثقافة التنظيمية تجاه تنفيذ أنظمة الأمن السيبراني.




**شكل ٣. نتائج تحليل الاعتدال للثقافة التنظيمية نحو نظام الأمن السيبراني**

## المناقشة والتوصيات

تشير نتائج الدراسة إلى أن إدراك موظفي المطارات السياحية لأهمية تنفيذ أنظمة الأمن السيبراني يؤثر بشكل كبير على الوعي المتصور لديهم تجاه تلك الأنظمة. وقد أظهرت نتائج الدراسة أن التعزيز الأمني لم يكن له تأثير معنوي على الوعي المتصور بنظام الأمن السيبراني، مما يشير إلى أن تحسين إجراءات التعزيز الأمني وحدها ليست كافية لتعزيز الوعي بين الموظفين. قد يكون السبب

في ذلك هو قلة التدريب أو التواصل الفعال حول هذه الإجراءات. تدعم هذه النتيجة دراسات سابقة تشير إلى أن التعزيز الأمني يحتاج إلى دعم بجهود توعوية وثقافية داخل المؤسسات لتحقيق نتائج ملموسة (Lykou et al.,2018 ).

كما أظهرت النتائج تأثيرًا إيجابيًا ومعنويًا للخصوصية الأمنية على الوعي المتصور، تعكس هذه النتائج أن الموظفين يقدّرون بشكل أكبر الجوانب المتعلقة بحماية الخصوصية وسرية البيانات مقارنة بجهود التعزيز الأمني. مما يتفق مع دراسة Liu et al.(2012) التي تؤكد أن الخصوصية الأمنية تعمل على تعزيز الثقة والوعي الأمني بين الموظفين وثقتهم في الأنظمة وتقلل من المخاطر المرتبطة بالتسريبات الأمنية. فحماية الخصوصية تعزز الشعور بالأمان لدى الموظفين، مما يزيد من التزامهم بالإجراءات الأمنية المتبعة.

كما بينت النتائج تأثيرًا إيجابيًا ومعنويًا لسرية البيانات على الوعي المتصور، وهذا يتماشى مع الأدبيات التي تبرز أهمية سرية البيانات في الحفاظ على أمن المعلومات وتعزيز الوعي السيبرانى. تعزيز سرية البيانات يساهم في بناء بيئة عمل آمنة، مما يعزز الوعي بين الموظفين بأهمية الإجراءات الأمنية، وهو ما يتفق مع(2022) Czuryk الذي يؤكد على ان الموظفين الذين يشعرون بأن معلوماتهم الشخصية والمهنية محمية يكونون أكثر وعيًا بأهمية الالتزام بإجراءات الأمن السيبراني.

أثبتت الدراسة أن الثقافة التنظيمية لها تأثير إيجابي ومعنوي على الوعي المتصور بنظام الأمن السيبراني، مما يدعم نتائج الأبحاث السابقة التي تؤكد على دور الثقافة التنظيمية في تعزيز الوعي الأمني (Hasan et al.,2021;Georgiadou et al.,2022) .. تساهم الثقافة التنظيمية القوية في تعزيز الالتزام بالإجراءات الأمنية وتطبيقها بشكل فعال.

بالإضافة إلى ذلك، بينت النتائج أن الثقافة التنظيمية تعزز تأثير الخصوصية الأمنية وسرية البيانات على الوعي المتصور، مما يبرز أهمية تبني ثقافة تنظيمية قوية تدعم تنفيذ أنظمة الأمن السيبراني لتحقيق أفضل النتائج في حماية البيانات وتعزيز الوعي الأمني. لكنها لم تؤثر بشكل معنوي على العلاقة بين التعزيز الأمني والوعي المتصور، وهذا يشير إلى أن التعزيز الأمني بحد ذاته قد لا يكون كافيًا لتحفيز وعي الموظفين إذا لم يكن مصحوبًا بإجراءات واضحة وفعالة لحماية الخصوصية وسرية البيانات. هذا التفسير يوضح لماذا لم يظهر التعزيز الأمني تأثيرًا معنويًا في نتائج الدراسة.

**التوصيات**

بناءً على النتائج المستخلصة، يمكن تقديم التوصيات التالية إلى وزارة الطيران المدني ممثلةً في مديري المطارات المصرية لتعزيز تنفيذ أنظمة الأمن السيبراني:

- تهيئة بيئة العمل وتطوير الثقافة التنظيمية التي تركز على الأمن السيبراني. لذلك، يجب دمج أبعاد ومبادئ الأمن السيبراني بشكل استراتيجي في القيم الأساسية في إدارات المطارات. يمكن تحقيق هذا التكامل من خلال تعزيز التواصل الداخلي، ووضع سياسات محددة وقابلة للتنفيذ والتحديث باستمرار لمواكبة التقدم التكنولوجي لأنواع وأشكال الهجمات السيبرانية، على أن يتم التأكد من دراية جميع الموظفين بهذه السياسات. كما يجب تحديد أهداف استراتيجية تدعم الأمن السيبراني بشكل فعال على كافة المستويات الإدارية. هذا ويتحتم التأكيد على امتثال الإدارة العليا بإظهار التزامها القوى بمعايير تطبيق أبعاد الأمن السيبراني على أن يكون هذا الالتزام واضحاً ومتسقا وموجهاً للموظفين بأكملهم.
- يجب على إدارات المطارات تعزيز الثقافة السيبرانية داخل بيئة عمل المطارات، ليكون الأمن السيبراني جزءًا من الثقافة التنظيمية. يمكن تحقيق ذلك من خلال نشر ثقافة المواطنة والنظافة الرقمية بين موظفي المطارات لخلق بيئة تنافسية آمنة في مطارات مصر السياحية. مع التركيز علي الجهود التوعوية والتدريبة من خلال تنظيم ورش عمل وإطلاق الدورات

التدريبية التي تركز على رفع الوعي بأهمية الأمن السيبراني بين الموظفين وفهمهم للتهديدات السيبرانية وكيفية التعامل معها بفعالية. فضلاً عن زيادة برامج التدريب المتخصصة المنوطة بمختلف جوانب الأمن السيبراني، المصممة خصيصًا لتناسب أدوار ومسؤوليات الموظفين المختلفة داخل المطارات.

- لابد من تعزيز التواصل المفتوح حول تهديدات الأمن السيبراني وأفضل الممارسات، فيجب أن يشعر موظفو المطارات بالراحة في الإبلاغ عن المشكلات الأمنية المحتملة دون خوف من الإدارة. هذا بالإضافة إلى تمكين الموظفين من المشاركة في مبادرات الأمن السيبراني وإشراكهم في وضع وتطوير وتنفيذ السياسات والإجراءات الأمنية.

- تعزيز التعلم المستمر من خلال التحديث المنتظم والدورات التجديدية، فالأمن السيبراني هو مجال ديناميكي، والبقاء على اطلاع دائم بأحدث التهديدات والتقنيات أمر بالغ الأهمية. مع إجراء محاكاة للهجمات الإلكترونية (على سبيل المثال، محاكاة التصيد الاحتيالي) لتقييم وتحسين استجابة الموظفين. يمكن أن تساعد هذه التمارين في تحديد نقاط الضعف وتعزيز التدريب. كما يجب إنشاء ونشر خطط استجابة للحوادث والهجمات السيبرانية حتى يعرف الموظفون الخطوات التي يجب اتخاذها والأشخاص المعنيين في حالة حدوث حادث للأمن السيبراني.

- من المهم أن تضع إدارات المطارات سياسات أمنية صارمة وشفافة، تشمل تعليمات دقيقة لحماية البيانات الحساسة والتعامل مع تبادل المعلومات السرية، يجب أن تكون هذه السياسات متاحة لجميع الموظفين وتُعاد تقييمها ومراجعتها بصفة دورية، وتحديثها بانتظام لمواكبة التقنيات الجديدة والتهديدات السيبرانية المتطورة. كما يتحتم التركيز على تعزيز إجراءات الخصوصية الأمنية وسرية البيانات، حيث أظهرت النتائج أن لهذه العوامل تأثير كبير على وعي الموظفين. يمكن تحقيق ذلك من خلال اعتماد تقنيات حديثة للمصادقة والتشفير، وتحديث جدران الحماية بشكل مستمر. بالإضافة إلى تنفيذ برامج مكافحة الفيروسات المرخصة والتحديث المستمر لها لضمان حماية الأنظمة من البرمجيات الخبيثة.

- ينبغي على إدارة المطارات زيادة الاستثمارات في البنية التحتية الأمنية و تخصيص ميزانيات أكبر لتطوير الحلول الأمنية المتقدمة، والتقنيات الجديدة لكشف ومراقبة التهديدات السيبرانية بشكل مستمر، مما يعزز من قدرتها على مواجهة التحديات الأمنية الحديثة.

- تشجيع ومكافأة أفضل الممارسات للموظفين الذين يظهرون التزامًا قويًا بالأمن السيبراني مثل اتباع سياسات كلمات المرور القوية والتصفح الآمن والتحديثات البرمجية المنتظمة.

- تعزيز الشعور الجماعي بالمسئولية من خلال تيسير التعلم من النظير للنظير وتبادل المعارف والتجارب والرؤى بين الموظفين. مع تحديد آليات لجمع آراء واقتراحات الموظفين حول تحسين الممارسات الأمنية.

- ينبغي على إدارات المطارات التعاون مع خبراء الأمن السيبراني للحصول على الاستشارات المتخصصة بغرض تطوير الإستراتيجيات الأمنية الفعالة، بالإضافة إلى ذلك، يمكن إقامة شراكات مع شركات الأمن السيبراني لتوفير حلول تقنية متطورة ومتكاملة والاستفادة من خبراتهم لتقديم حلول مخصصة تتناسب مع احتياجات المطارات السياحية الخاصة. كما يجب التوجه للإنضمام لكافة المنظمات المعنية بمجال حماية الأمن المعلوماتي والسيبراني للإستفادة من التجارب الدولية في هذا المجال.

- من الضروري أن تقوم إدارات المطارات بإجراء تقييمات دورية لأداء أنظمة الأمن السيبراني. يتضمن ذلك تحليل مدى فعالية السياسات والتدابير المتخذة والتأكد من ملائمتها لأحدث المعايير الأمنية، ليتم تحسين الأداء العام للأمن السيبراني في المطارات، وتعديل الاستراتيجيات الأمنية بناءً على نتائج التقييمات والتحليلات المستمرة.

- تطوير آليات الرصد والمراقبة من خلال إنشاء فرق متخصصة لمراقبة الأنظمة والشبكات بشكل مستمر للكشف عن أي نشاط غير طبيعي أو اختراقات محتملة. كذلك استخدام أدوات تحليل البيانات الكبيرة لتحليل الأنماط والتنبؤ بالتهديدات السيبرانية قبل حدوثهاTop of Form.

- نظراً لما يواجه قطاع الطيران المدني من تهديدات سيبرانية عابرة للحدود، فيجب التأكيد على أهمية إقرار استراتيجيات وطنية مشتركة. بما يتطلب تطوير بنية تحتية رقمية آمنة لتعزيز حماية أنظمة هذا القطاع الحيوي وشبكاته. كما ينبغي توفير دفاعات قوية للطائرات والمطارات، وتحديد الثغرات المحتملة وتأمينها بشكل استباقي. وعلى الرغم من أن النتائج أظهرت عدم تأثير التعزيز الأمني بشكل معنوي، إلا أن تحسين آليات التعزيز الأمني يمكن أن يساهم في تحسين تنفيذ أنظمة الأمن السيبراني بشكل عام من خلال تبني تقنيات حديثة لمراقبة البيانات وتحديد المخترق منها مع تطوير آليات الاستجابة وأنظمة الإنذار المبكر لاكتشاف ومنع المخاطر التقنية.

- لابد من توجيه توصية لوزارات التعليم العالي، والتربية والتعليم، بالتعاون مع السياحة والآثار. لتعزيز القدرات الوطنية المتعلقة بالمهارات البشرية للعاملين في صناعة السياحة والطيران، لتكون خطوة استراتيجية هامة بما يشمل تطوير المناهج الدراسية في كليات ومعاهد ومدارس السياحة والفنادق ودمج مواضيع أمن وحماية المعلومات في هذه المناهج.

وفي النهاية، من خلال تعزيز الثقافة التنظيمية التي تولي الأمن السيبراني أولوية، وتهتم بمشاركة الموظفين في جهود التوعية والتنفيذ، يمكن للمطارات السياحية تعزيز موقفها نحو الأمن السيبراني بشكل كبير. هذا النهج الشامل لا يحمى الأنظمة والبيانات المهمة للمسافرين فحسب، بل يمكّن الموظفين أيضًا من توخي الحذر وإتخاذ الإجراءات الاستباقية في التصدى للتهديدات الإلكترونية.

## قائمة المراجع

### أولًا: المراجع العربية


البيشي، منير عبد الله مفلح (٢٠٢١). الأمن السيبراني في الجامعات السعودية و أثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس: دراسة على جامعة بيشة، *مجلة الجامعة الإسلامية للدراسات التربوية و النفسية*، مجلد ٢٩، عدد ٦، ص ص: ٣٥٣-٣٧٢

الزهراني، عبدالله يحي سعيد (٢٠٢٠). استراتيجيات الأمن السيبراني في ضوء التقنيات والتحديات الحديثة: دراسة مقارنة، رسالة دكتوراة، قسم الدراسات الاستراتيجية، جامعة نايف العربية للعلوم الأمنية، السعودية.

السمحان، منى عبدالله (٢٠٢٠)، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، *مجلة كلية التربية*، العدد(١١١)،جامعة المنصورة، ص ص:٣-٢٩.

المري، راشد محمد (٢٠٢٣)، الأمن السيبراني وحماية الأنظمة الإلكترونية دراسة تحليلية تأصيلية. *مجلة الدراسات القانونية والاقتصادية*، ٩(١)،٩٥٩-١٠٠٨.

حمود، رافد عباس (٢٠٢٣)، تأثير الأمن السيبراني على أداء المنظمة: دراسة استطلاعية لآراء عينة من العاملين في شركة ايرثلنك، الدبلوم العالي في إدارة الجودة، كلية الإدارة والاقتصاد، قسم إدارة الأعمال، جامعة كربلاء، العراق.

على إبراهيم أحمد, فاطمة؛ يوسف, رحاب؛ السيد، وليد محمود،(٢٠٢٢). الأمن السيبراني والنظافة الرقمية، *المجلة المصرية لعلوم المعلومات*، مج(٩)، ع(٢)،ص ص: ٣٩٠-٤٢٢.

وزارة الطيران المدني المصرية، المركز الإعلامي،تقرير محاولة اختراق موقع شركة ميناء القاهرة الجوي الإلكتروني،٢٠٢٣ .

وزارة الطيران المدني المصرية، الشركة المصرية القابضة للمطارات والملاحة الجوية، التقرير السنوي، ٢٠٢٣.

Abdel-Al, A.J., Al-Saeed F., S., & Atwa A., R. (2022). Egyptian efforts to face cyber challenges. *Scientific Journal of Environmental Studies*, 13(2), 265-286.

Abd El-Maksoud,R. (2024). Exploring the role of cybersecurity in enhancing digital trust of Egyptian travel agencies. *Journal of Association of Arab Universities for Tourism and Hospitality*, 26(1), 185-204.

Abeyratne, R. (2016). Aviation Cyber Security: A Constructive Look at the Work of ICAO. *Air and Space Law*, 41(1).

Abeyratne, R. (2020). Aviation and cybersecurity in the digital world. Aviation in the Digital Age: Legal and Regulatory Aspects, 173-211.

Aboti, C. D. (2019). Survey on IoT: Challenges and cyber risks in commercial aviation. *IJRAR*, 6(2), 1-9.

Ahmed, E. M. (2021). Modelling information and communications technology cyber security externalities spillover effects on sustainable economic growth. *Journal of the Knowledge Economy*, 12(1), 412-430.

Aksoy, C. (2024). Buliding A Cyber Security Culture For Resilient Organization Aganist Cyber Attacks. *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*, 7(1), 96-110.

Alabsi, M. I., & Gill, A. Q. (2021). A Review of Passenger Digital Information Privacy Concerns in Smart Airports. *IEEE Access*, 9, 33769-33781.

Alansari, Z., Soomro, S., & Belgaum, M. R. (2019). Smart airports: Review and open research issues. In Emerging Technologies in Computing: Second International Conference, iCETiC 2019, London, UK, August 19–20, 2019, Proceedings 2 (pp. 136-148). *Springer International Publishing*.

Albataineh, A., & Alsmadi, I. (2019, June). Iot and the risk of internet exposure: Risk assessment using shodan queries. In 2019 IEEE 20th International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM),pp. 1-5.

Alladi, T., Chamola, V., Sikdar, B., & Choo, K. K. R. (2020). Consumer IoT: Security vulnerability case studies and solutions. *IEEE Consumer Electronics Magazine*, 9(2), 17-25.

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of advances in information technology*, 3(3), 176-183.

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333.

Beecroft, M. (2019). The future security of travel by public transport: A review of evidence. *Research in Transportation Business & Management*, 32, 100388.

Berlilana, Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini. (2021). Organization benefit as an outcome of organizational security adoption: The role of cyber security readiness and technology readiness. *Sustainability*, 13(24), 13761.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 523-548.

Chen, H. S., & Fiscus, J. (2018). The inhospitable vulnerability: A need for cybersecurity risk assessment in the hospitality industry. *Journal of Hospitality and Tourism Technology*, 9(2), 223-234.

Chiappetta, A., & Cuozzo, G. (2017). Critical infrastructure protection: Beyond the hybrid port and airport firmware security cybersecurity applications on transport. In 2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS),pp. 206-211.

Choi, S.E., Martins, J.T.&Bernik, I. (2018). Information Security: Listening to the perspective of organisational insiders. *Journal of Information Science*,44(1),٤٣-١.

Corallo, A., Lazoi, M., Lezzi, M., & Pontrandolfo, P. (2021). Cybersecurity challenges for manufacturing systems 4.0: assessment of the business impact level. *IEEE Transactions on Engineering Management*, 70(11), 3745-3765.

Czuryk, M. (2022). Restrictions on the exercising of human and civil rights and freedoms due to cybersecurity issues. Studia Iuridica Lublinensia, 31(3), 31-43.

Daud, M., Rasiah, R., George, M., Asirvatham, D., & Thangiah, G. (2018). Bridging the gap between organisational practices and cyber security compliance: can cooperation promote compliance in organisations?. *International Journal of Business & Society*, 19(1).

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, 11(10), 4580.

Eilts, D. (2020). An empirical assessment of cybersecurity readiness and resilience in small businesses.Ph.D. Thesis, Nova Southeastern University, Fort Lauderdale, FL, USA.

Elmarady, A. A., & Rahouma, K. (2021). Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assessment. IEEE access, 9, 143997-144016.

Gallegos-Segovia, P. L., Bravo-Torres, J. F., Argudo-Parra, J. J., Sacoto-Cabrera, E. J., & Larios-Rosillo, V. M. (2017, June). Internet of things as an attack vector to critical infrastructures of cities. In 2017 International Caribbean Conference on Devices, Circuits and Systems (ICCDCS), pp. 117-120.

George, A. S., George, A. H., & Baskar, T. (2023). Digitally immune systems: building robust defences in the age of cyber threats. Partners Universal International Innovation Journal, 1(4), 155-172.

George, G., & Thampi, S. M. (2019). Vulnerability-based risk assessment and mitigation strategies for edge devices in the Internet of Things. Pervasive and Mobile Computing, 59, 101068.

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, 62(3), 452-462.

Guenther, P., Guenther, M., Ringle, C. M., Zaefarian, G., & Cartwright, S. (2023). Improving PLS-SEM use for business marketing research. *Industrial Marketing Management*, 111, 127-142.

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer networks, 169, 107094.

Hair, J. F., Matthews, L. M., Matthews, R. L., & Sarstedt, M. (2017). PLS-SEM or CB-SEM: Updated guidelines on which method to use. *International Journal of Multivariate Data Analysis*, 1(2), 107-123.

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

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, 58, 102726.

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics*, 3(5), 97.

Iasiello, E. (2013). Getting ahead of the threat: Aviation and cyber security. *Aerospace America*, 51(7), 22-25.

Jeyakodi, D. (2015). Cyber security in civil aviation. *The Aviation and Space Journal*, 14(4), 2-9.

Kharlamov, A., & Pogrebna, G. (2021). Using human values-based approach to understand cross-cultural commitment toward regulation and governance of cybersecurity. *Regulation & Governance*, 15(3), 709-724.

Kim, D., & Solomon, M. G. (2010). Fundamentals of information systems security. Jones & Bartlett Publishers.

Klenka, M. (2021). Aviation cyber security: legal aspects of cyber threats. *Journal of transportation security*, 14(3), 177-195.

Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P., & Janicke, H. (2020). A holistic review of cybersecurity and reliability perspectives in smart airports. IEEE Access, 8, 209802-209834.

Kovacic,M., Cicin-Sain,M.,&Milojica,V.(2022). Cyber Security and Tourism: Biblomitric Analysis. *Journal of Process Management New Technologies*, 10(3-4),75-92.

Kurt, M. N., Yılmaz, Y., & Wang, X. (2018). Real-time detection of hybrid and stealthy cyber-attacks in smart grid. IEEE Transactions on Information Forensics and Security, 14(2), 498-513.

Lehto, M. (2020). Cyber security in aviation, maritime and automotive. Computation and Big Data for Transport: Digital Innovations in Surface and Air Transport Systems, 19-32.

Lekota, F., & Coetzee, M. (2019). Cybersecurity incident response for the sub-saharan African aviation industry. In International Conference on Cyber Warfare and Security (pp. 536-XII). Academic Conferences International Limited.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45, 13-24.

Liu, J., Xiao, Y., Li, S., Liang, W., & Chen, C. P. (2012). Cyber security and privacy issues in smart grids. IEEE Communications surveys & tutorials, 14(4), 981-997.

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018). Smart airport cybersecurity: Threat mitigation and cyber resilience controls. Sensors, 19(1), 19.

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018, June). Implementing cyber-security measures in airports to improve cyber-resilience. In 2018 Global Internet of Things Summit (GIoTS), pp. 1-6.

Lykou, G., Moustakas, D., & Gritzalis, D. (2020). Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies. Sensors, 20(12), 3537.

Memon, M. A., Ramayah, T., Cheah, J. H., Ting, H., Chuah, F., & Cham, T. H. (2021). PLS-SEM statistical programs: A review. *Journal of Applied Structural Equation Modeling*, 5(1), 1-14.

Marcial, D.E.,&Launer,M.A. (2019).Towards the Measurement of Digital Trust in the Workplace: A Proposed Framework. *International Journal of Scientific Engineering and Science*,3(12),1-7.

Nobles, C. (2019). Cyber threats in civil aviation. In Emergency and Disaster Management: Concepts, Methodologies, Tools, and Applications, pp. 119-141.

Paraskevas, A. (2022). Cybersecurity in travel and tourism: A risk-based approach. In Handbook of e-Tourism (pp. 1605-1628). Cham: Springer International Publishing.

Pearson, N. (2014). A larger problem: financial and reputational risks. *Computer Fraud & Security*, 2014(4), 11-13.

Pierides, M. (2015). Cybersecurity and the aviation sector: Recent incidents highlight unique risks. Pillsbury Law.

Rajapaksha, A., & Jayasuriya, N. (2020). Smart airport: A review on future of the airport operation. *Global Journal of Management and Business Research*, 20(3), 25-34.

Rîndașu, S. M. (2017). Emerging information technologies in accounting and related security risks–what is the impact on the Romanian accounting profession. *Journal of Accounting and Management Information Systems*, 16(4), 581-609.

Sarstedt, M., Radomir, L., Moisescu, O. I., & Ringle, C. M. (2022). Latent class analysis in PLS-SEM: A review and recommendations for future applications. *Journal of Business Research*, 138, 398-407.

Sarstedt, M., Ringle, C. M., Cheah, J. H., Ting, H., Moisescu, O. I., & Radomir, L. (2020). Structural model robustness checks in PLS-SEM. *Tourism Economics*, 26(4), 531-554.

Shukla, S., George, J. P., Tiwari, K., & Kureethara, J. V. (2022). Data security. In Data Ethics and Challenges, Singapore: Springer Singapore,pp. 41-59.

Suciu, G., Scheianu, A., Petre, I., Chiva, L., & Bosoc, C. S. (2019, March). Cybersecurity threats analysis for airports. In World Conference on Information Systems and Technologies (pp. 252-262). Cham: Springer International Publishing.

Suciu, G., Scheianu, A., Vulpe, A., Petre, I., & Suciu, V. (2018). Cyber-attacks–the impact over airports security and prevention modalities. In Trends and Advances in Information Systems and Technologies: Volume 36, Springer International Publishing, pp. 154-162.

Tejay, G. P., & Mohammed, Z. A. (2023). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. *Information & Management*, 60(3), 103751.

Trim, P. R., & Lee, Y. I. (2019). The role of B2B marketers in increasing cyber security awareness and influencing behavioural change. *Industrial Marketing Management Journal*, 83, 224-238.

Usama, M., Ullah, U., & Sajid, A. (2024). Cyber Attacks Against Intelligent Transportation Systems. In Cyber Security for Next-Generation Computing Technologies (pp. 190-230). CRC Press.

Willemsen, B., & Cadee, M. (2018). Extending the airport boundary: Connecting physical security and cybersecurity. *Journal of Airport Management*, 12(3), 236-247.

Wong, L. W., Lee, V. H., Tan, G. W. H., Ooi, K. B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, 66, 102520.