

فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية في
ضوء التحول الرقمي

إعداد الطالب/

مشاري علي العريني

الرقم الجامعي/

٢٥٣.٠.١١٥

إشراف/

أ.د. الفيصل عبد الحميد محمد حسن

أ.د. فايز جراد

العام الدراسي

٢٠٢٦ م

وقل رب زدني علما

إهداء

إلى من غرس في القيم، وسقاني من معين الحكمة،

إلى من كان دعاؤهم سرّ توفيقِي، وسنداً لي في كل مراحل حياتي،

إلى والديّ الكريمين، أهدي ثمرة جهدي وعملي، عرفاناً وتقديرًا.

وإلى من ساندني وشجّعني في مسيرتي العلمية،

إلى إخوتي وأصدقائي وزملائي،

لكم جميعًا أهدي هذا العمل المتواضع، امتنانًا لكل دعم صادق.

شكر وتقدير

الحمد لله الذي بنعمته تتم الصالحات، وبِعونه وتوفيقه أنجزت هذا العمل المتواضع.

أتقدم بخالص الشكر وعظيم الامتنان لمُشرفي الكريم الأستاذ الدكتور د. الفيصل عبد الحميد، د. فايز جرادة، الذي كان لدعمها العلمي، وتوجيهاتهم السديدة، وملاحظاتهم القيمة، الأثر الأكبر في إنجاز هذه الرسالة. لقد كان مثلاً يُحتذى به في العلم والأخلاق والتفاني.

كما أتوجه بالشكر الجزيل لأعضاء لجنة المناقشة الكرام على وقتهم وجهدهم وملاحظاتهم البناءة التي أثرت هذا العمل.

ولا يفوتني أن أعبر عن تقديري العميق لكل من ساندني ووقف إلى جانبي خلال فترة إعداد

الرسالة، من أسرتي وأصدقائي وزملائي، وخاصة والدي العزيزين، الذين كان لدعائهما

ودعمهما المعنوي والمادي بالغ الأثر في وصولي إلى هذه المرحلة.

لكم جميعاً، كل الشكر والتقدير والامتنان.

فهرس المحتويات

٣	إهداء
٤	شكر وتقدير
٧	قائمة الجداول
٩	فهرس الأشكال
١١	المستخلص
١٢	الفصل الأول
١٣	المقدمة
١٤	مشكلة الدراسة
١٥	أهمية الدراسة
١٦	أهداف الدراسة
١٦	تساؤلات الدراسة
١٧	فرضيات الدراسة
١٧	النظرية العلمية المتبعة لإعداد البحث
٢١	الفصل الثاني
٢١	الدراسات السابقة
٢٢	المقدمة
٢٣	المتغير التابع والمستقل
٢٦	الدراسات السابقة
٣٠	المنطلقات النظرية للدراسة
٣٢	الفصل الثالث
٣٢	منهجية الدراسة
٣٣	المقدمة
٣٤	مجتمع البحث
٣٥	المنهجية وطرق البحث

٣٦	خطوات جمع البيانات
٣٩	أدوات الدراسة
٤٠	حدود البحث
٤٢	الفصل الرابع
٤٢	نتائج الدراسة
٤٣	المقدمة
٤٤	تحليل البيانات
٩٧	المناقشة
٩٩	الخاتمة
١٠٠	التوصيات
١٠١	المراجع
١٠٤	الملاحق
١٠٩	Abstract

قائمة الجداول

٤٤	جدول ١: التحليلات الإحصائية
٤٧	جدول ٢: التحليل الإحصائي للعمر
٤٩	جدول ٣: التحليل الإحصائي للجنس
٥٠	جدول ٤: التحليل الإحصائي للدرجة العلمية
٥٢	جدول ٥: التحليل الإحصائي لتطبيق الجهة الحكومية استراتيجيات واضحة لإدارة مخاطر الأمن السيبراني
٥٤	جدول ٦: التحليل الإحصائي لتحديث استراتيجيات الأمن السيبراني بشكل دوري لمواكبة التهديدات الحديثة
٥٦	جدول ٧: التحليل الإحصائي لاعتماد الجهة على منهجيات علمية لتحديد وتقييم المخاطر السيبرانية
٥٨	جدول ٨: التحليل الإحصائي لمساهمة استراتيجيات إدارة المخاطر في تقليل احتمالية وقوع الهجمات السيبرانية
٦٠	جدول ٩: التحليل الإحصائي لمساعدة استراتيجيات الأمن السيبراني في ضمان استمرارية الأعمال والخدمات الحكومية
٦٢	جدول ١٠: التحليل الإحصائي لمساهمة تطبيق استراتيجيات إدارة المخاطر في تعزيز أمن البيئة الرقمية للجهة
٦٤	جدول ١١: التحليل الإحصائي لامتلاك الجهة بنية تقنية متطورة لدعم الأمن السيبراني
٦٦	جدول ١٢: التحليل الإحصائي لاستخدام الجهة تقنيات حديثة لرصد واكتشاف التهديدات السيبرانية
٦٨	جدول ١٣: التحليل الإحصائي لتحديث الأنظمة الأمنية بصورة مستمرة لمواجهة المخاطر الجديدة
٧٠	جدول ١٤: التحليل الإحصائي لمساهمة البنية التقنية في رفع كفاءة الاستجابة للحوادث السيبرانية
٧٢	جدول ١٥: التحليل الإحصائي لمساعدة الأنظمة التقنية المتقدمة في حماية البيانات والأصول الرقمية
٧٤	جدول ١٦: التحليل الإحصائي لمساهمة الجاهزية التقنية في تعزيز فعالية إدارة مخاطر الأمن السيبراني
٧٦	جدول ١٧: التحليل الإحصائي لتوفير الجهة برامج تدريبية منتظمة في مجال الأمن السيبراني للعاملين
٧٧	جدول ١٨: التحليل الإحصائي لنشر الوعي بالمخاطر السيبرانية بين جميع الموظفين
٧٩	جدول ١٩: التحليل الإحصائي لالتزام العاملون بتطبيق سياسات وإجراءات الأمن السيبراني
٨١	جدول ٢٠: التحليل الإحصائي لمساهمة التدريب والتوعية في الحد من الأخطاء البشرية المرتبطة بالأمن السيبراني
	جدول ٢١: التحليل الإحصائي لمساهمة استراتيجيات إدارة مخاطر الأمن السيبراني في تعزيز فعالية إدارة المخاطر في الجهات الحكومية بالملكة العربية السعودية في ضوء التحول الرقمي
٨٢	
٨٤	جدول ٢٢: ملخص التحليلات الإحصائية
٨٤	جدول ٢٣: اختيار النيات والمؤثوقية
	جدول ٢٤: اختبار كاي اسكورير للعلاقة بين فعالية إدارة مخاطر الأمن السيبراني في الجهات الحكومية وتطبيق استراتيجيات إدارة مخاطر الأمن السيبراني
٨٦	
	جدول ٢٥: اختبار كاي اسكورير للعلاقة بين فعالية إدارة مخاطر الأمن السيبراني في الجهات الحكومية والجاهزية التقنية
٨٨	وبنية الأمن السيبراني

جدول ٢٦ : اختبار كاي اسكور للعلاقة بين فعالية إدارة مخاطر الأمن السيبراني في الجهات الحكومية. والتوعية والتدريب في مجال الأمن السيبراني.....	٩٠
جدول ٢٧ : ملخص النموذج.....	٩٢
جدول ٢٨ : تحليل التباين.....	٩٢
جدول ٢٩ : معاملات تحليل الانحدار المتعدد.....	٩٢
جدول ٣٠ : اختبار التباين الأحادي.....	٩٥
جدول ٣١ : ملخص نموذج معامل بايز.....	٩٥

فهرس الأخطال

٤٨	شكل توضيحي ١: التمثيل البياني للعمر
٤٩	شكل توضيحي ٢: التمثيل البياني للجنس
٥١	شكل توضيحي ٣: التمثيل البياني للدرجة العلمية
٥٣	شكل توضيحي ٤: التمثيل البياني لتطبيق الجهة الحكومية استراتيجيات واضحة لإدارة مخاطر الأمن السيبراني
٥٥	شكل توضيحي ٥: التمثيل البياني لتحديث استراتيجيات الأمن السيبراني بشكل دوري لمواكبة التهديدات الحديثة
٥٧	شكل توضيحي ٦: التمثيل البياني لاعتماد الجهة على منهجيات علمية لتحديد وتقييم المخاطر السيبرانية
٥٩	شكل توضيحي ٧: التمثيل البياني لمساهمة استراتيجيات إدارة المخاطر في تقليل احتمالية وقوع الهجمات السيبرانية
٦١	شكل توضيحي ٨: التمثيل البياني لمساعدة استراتيجيات الأمن السيبراني في ضمان استمرارية الأعمال والخدمات الحكومية
٦٣	شكل توضيحي ٩: التمثيل البياني لمساهمة تطبيق استراتيجيات إدارة المخاطر في تعزيز أمن البيئة الرقمية للجهة
٦٥	شكل توضيحي ١٠: التمثيل البياني لامتلاك الجهة بنية تقنية متطورة لدعم الأمن السيبراني
٦٧	شكل توضيحي ١١: التمثيل البياني لاستخدام الجهة تقنيات حديثة لرصد واكتشاف التهديدات السيبرانية
٦٩	شكل توضيحي ١٢: التمثيل البياني لتحديث الأنظمة الأمنية بصورة مستمرة لمواجهة المخاطر الجديدة
٧١	شكل توضيحي ١٣: التمثيل البياني لمساهمة البنية التقنية في رفع كفاءة الاستجابة للحوادث السيبرانية
٧٣	شكل توضيحي ١٤: التمثيل البياني لمساعدة الأنظمة التقنية المتقدمة في حماية البيانات والأصول الرقمية
٧٥	شكل توضيحي ١٥: التمثيل البياني لمساهمة الجاهزية التقنية في تعزيز فعالية إدارة مخاطر الأمن السيبراني
٧٦	شكل توضيحي ١٦: التمثيل البياني لتوفير الجهة برامج تدريبية منتظمة في مجال الأمن السيبراني للعاملين
٧٨	شكل توضيحي ١٧: التمثيل البياني لنشر الوعي بالمخاطر السيبرانية بين جميع الموظفين
٨٠	شكل توضيحي ١٨: التمثيل البياني لالتزام العاملون بتطبيق سياسات وإجراءات الأمن السيبراني
٨١	شكل توضيحي ١٩: التمثيل البياني لمساهمة التدريب والتوعية في الحد من الأخطاء البشرية المرتبطة بالأمن السيبراني
	شكل توضيحي ٢٠: التمثيل البياني لمساهمة استراتيجيات إدارة مخاطر الأمن السيبراني في تعزيز فعالية إدارة المخاطر في
٨٣	الجهات الحكومية بالمملكة العربية السعودية في ضوء التحول الرقمي
٨٥	شكل توضيحي ٢١: متغيرات الدراسة التابعة والمستقلة
	شكل توضيحي ٢٢: المقاييس المتماثلة لتحليل الجداول المتقاطعة للعلاقة بين فعالية إدارة مخاطر الأمن السيبراني في الجهات
٨٧	الحكومية. وتطبيق استراتيجيات إدارة مخاطر الأمن السيبراني
	شكل توضيحي ٢٣: المقاييس المتماثلة لتحليل الجداول المتقاطعة للعلاقة بين فعالية إدارة مخاطر الأمن السيبراني في الجهات
٨٩	الحكومية. والجاهزية التقنية وبنية الأمن السيبراني
	شكل توضيحي ٢٤: المقاييس المتماثلة لتحليل الجداول المتقاطعة للعلاقة بين فعالية إدارة مخاطر الأمن السيبراني في الجهات
٩١	الحكومية. والتوعية والتدريب في مجال الأمن السيبراني
٩٣	شكل توضيحي ٢٥: شكل الانتشار للبواق

شكل توضيحي ٢٦ : مصغوفة شكل الانتشار ٩٤

المستخلص

هدفت هذه الدراسة إلى التعرف على فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية في ضوء التحول الرقمي، من خلال قياس أثر تطبيق استراتيجيات إدارة مخاطر الأمن السيبراني، والجاهزية التقنية وبناء الأمن السيبراني، والتوعية والتدريب في مجال الأمن السيبراني في تعزيز فعالية إدارة مخاطر الأمن السيبراني داخل الجهات الحكومية. واعتمدت الدراسة على المنهج الكمي باستخدام الاستبانة بوصفها أداة رئيسة لجمع البيانات، وتم تطبيقها على عينة بلغت ٢٦٣ مشاركاً من العاملين في الجهات الحكومية ذات العلاقة بالأمن السيبراني وتقنية المعلومات وإدارة المخاطر، ثم جرى تحليل البيانات باستخدام الأساليب الإحصائية المناسبة لاختبار فرضيات الدراسة وتحقيق أهدافها. وأظهرت النتائج وجود أثر إيجابي ذي دلالة إحصائية للمتغيرات المستقلة في تعزيز فعالية إدارة مخاطر الأمن السيبراني. كما تبين أن تطبيق استراتيجيات إدارة المخاطر يمثل العامل الأكثر تأثيراً، يليه مستوى الجاهزية التقنية وبناء الأمن السيبراني، ثم برامج التوعية والتدريب الأمني. وأكدت النتائج أن التكامل بين الجوانب الإدارية والتقنية والبشرية يسهم في رفع جاهزية الجهات الحكومية لمواجهة التهديدات الإلكترونية، وتعزيز حماية البيانات واستمرارية الخدمات الرقمية، ودعم نجاح برامج التحول الرقمي. وأوصت الدراسة بضرورة تطوير استراتيجيات إدارة مخاطر الأمن السيبراني بصورة مستمرة، والاستثمار في تحديث البنية التحتية الأمنية، وتوسيع برامج التدريب والتوعية، وتطبيق الأطر والمعايير الدولية في إدارة المخاطر، وتعزيز استخدام التقنيات الذكية في اكتشاف التهديدات، إلى جانب إجراء تقييمات دورية لقياس فعالية الضوابط الأمنية وتحسينها بما يواكب التطورات التقنية والتهديدات السيبرانية المتجددة.

الكلمات المفتاحية: الأمن السيبراني، إدارة مخاطر الأمن السيبراني، التحول الرقمي، الجهات الحكومية، الجاهزية

التقنية، التوعية الأمنية، المملكة العربية السعودية.

الفصل الأول

المقدمة

يشهد العالم اليوم تحولات رقمية متسارعة أطلقت عصر الاعتماد المكثف على التقنيات الرقمية في جميع القطاعات، بما في ذلك الجهات الحكومية، حيث أصبحت الأنظمة الإلكترونية والخدمات الرقمية تشكل العمود الفقري لتقديم الخدمات للمواطنين والمستفيدين. وقد أدت هذه التحولات إلى تعزيز الكفاءة وسرعة الوصول إلى المعلومات، لكنها في الوقت ذاته خلقت تحديات جديدة مرتبطة بالأمن السيبراني، إذ أصبحت البيانات الحكومية والمعلومات الحساسة أكثر عرضة للتهديدات الإلكترونية والهجمات الرقمية المتطورة. ومن هذا المنطلق، باتت فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني قضية محورية لضمان استمرارية العمليات الحكومية وحماية المعلومات الحيوية، بما يعزز الثقة في الأنظمة الرقمية ويضمن تحقيق أهداف التحول الرقمي (Radebe, 2024).

تعتبر إدارة مخاطر الأمن السيبراني عملية شاملة تهدف إلى التعرف على التهديدات السيبرانية، تقييم مدى تأثيرها على الجهات الحكومية، ووضع الإجراءات الوقائية والتصحيحية للحد من تلك المخاطر. ويشمل ذلك تطوير سياسات أمنية متكاملة، تبني ضوابط تقنية وإدارية، وإجراء تقييم دوري للمخاطر لضمان قدرة الجهات الحكومية على الاستجابة السريعة لأي تهديد. وتشير الدراسات الحديثة إلى أن فاعلية هذه الاستراتيجيات تعتمد بشكل كبير على مدى دمجها مع أهداف التحول الرقمي، حيث تضمن الاستمرارية التشغيلية، حماية البيانات، والامتثال للمعايير الوطنية والدولية للأمن السيبراني (Melaku, 2023).

في المملكة العربية السعودية، أطلقت الحكومة برامج متعددة لتعزيز التحول الرقمي ضمن رؤية المملكة ٢٠٣٠، مما أدى إلى تبني حلول تقنية متقدمة في تقديم الخدمات العامة وربط الجهات الحكومية بأنظمة معلومات موحدة. ومع هذا التوسع الرقمي، برزت الحاجة إلى تطوير استراتيجيات إدارة مخاطر الأمن السيبراني بشكل يتماشى مع البيئة الرقمية الجديدة، بحيث لا تقتصر على الوقاية من الهجمات، بل تشمل أيضًا إدارة المخاطر التشغيلية، حماية المعلومات، وضمان استمرارية تقديم الخدمات الرقمية للمستفيدين. ومن هنا، تنبع أهمية هذه الدراسة في تسليط الضوء على فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية، وفهم مدى جاهزيتها لمواجهة التهديدات الرقمية المعقدة، وتحقيق التوازن بين التقدم الرقمي وحماية المعلومات الحساسة (Hossain, 2025). تهدف الدراسة إلى تقديم رؤية علمية وتحليلية تمكن الجهات الحكومية من تحسين استراتيجيات إدارة المخاطر السيبرانية، بما يساهم في تعزيز الثقة في التحول الرقمي، حماية الأصول المعلوماتية، وتحقيق الاستفادة القصوى من التقنية في تقديم الخدمات العامة. كما تسعى الدراسة إلى تحديد التحديات والمعوقات التي تواجه تنفيذ

هذه الاستراتيجيات، وتقديم توصيات عملية لتعزيز الفاعلية والكفاءة في مواجهة التهديدات السيبرانية الحديثة، بما يضمن استدامة الأمن الرقمي والمواءمة مع أهداف التنمية الوطنية.

مشكلة الدراسة

تواجه الجهات الحكومية في المملكة العربية السعودية تحديات متزايدة في مجال الأمن السيبراني نتيجة التحول الرقمي السريع الذي تشهده الدولة في إطار رؤية المملكة ٢٠٣٠. فالتوسع في استخدام الخدمات الرقمية، وأنظمة المعلومات الإلكترونية الموحدة، ورفع مستوى الاتصال الرقمي بين الجهات الحكومية والمستفيدين، على الرغم من فوائده الكبيرة في تحسين الكفاءة وجودة الخدمات، فإنه يعرض هذه الجهات لمخاطر سيبرانية متعددة تتراوح بين الاختراقات الأمنية، سرقة البيانات، الهجمات الإلكترونية المنظمة، وحتى التهديدات المتعلقة بالبرمجيات الخبيثة والهجمات على البنية التحتية الرقمية الحيوية. ونلاحظ أن بعض الجهات الحكومية لم تطبق استراتيجيات إدارة المخاطر السيبرانية بشكل شامل أو متكامل، مما يؤدي إلى فجوات في حماية البيانات وانخفاض القدرة على الاستجابة الفورية للتهديدات الرقمية، وبالتالي ضعف فاعلية النظام الرقمي بشكل عام.

ومن هنا، تنبع المشكلة الرئيسية للدراسة: ما مدى فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية في ضوء التحول الرقمي؟ إذ إن عدم كفاءة هذه الاستراتيجيات أو ضعف تطبيقها يمكن أن يؤدي إلى عدد من المشكلات المترتبة، أهمها:

- زيادة احتمالية التعرض للهجمات السيبرانية بسبب ضعف الإجراءات الوقائية وعدم تكامل الضوابط التقنية والإدارية.
- فقدان البيانات والمعلومات الحساسة ما يؤثر على الثقة في الخدمات الحكومية الرقمية ويهدد الخصوصية وحماية المواطنين.
- انقطاع أو تعطيل الخدمات الرقمية ما يؤدي إلى ضعف الأداء المؤسسي وتأخر تقديم الخدمات الحيوية للمستفيدين.
- ارتفاع التكاليف التشغيلية نتيجة استجابة الجهات الحكومية للأزمات الناتجة عن الهجمات السيبرانية أو التهديدات الأمنية.
- ضعف التوافق مع معايير الحوكمة والأمن السيبراني الوطنية والدولية، مما قد يعيق تحقيق أهداف التحول الرقمي وتعزيز الاستدامة الرقمية (Abn_hammad, ٢٠٢٥).

استنادًا إلى مشكلة الدراسة الرئيسية والمشكلات المترتبة عليها، يطرح البحث السؤال الرئيسي الذي يحدد محور الدراسة ويقود عملية التحليل والبحث العلمي: ما مدى فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية في ضوء التحول الرقمي، وما تأثير هذه الاستراتيجيات في حماية البيانات وضمان استمرارية تقديم الخدمات الرقمية؟

أهمية الدراسة

• الأهمية العلمية

تكتسب هذه الدراسة أهميتها العلمية من مساهمتها في توسيع المعرفة النظرية حول إدارة مخاطر الأمن السيبراني في القطاع الحكومي، خاصة في ظل التحول الرقمي المتسارع الذي تشهده المملكة العربية السعودية. إذ تمثل إدارة المخاطر السيبرانية عنصراً محورياً في ضمان استمرارية العمليات الرقمية وحماية البيانات الحكومية الحساسة، وبالتالي فهي تدخل ضمن الدراسات الحديثة في الإدارة العامة والأمن الرقمي. وتسعى الدراسة إلى تطوير إطار نظري متكامل يربط بين استراتيجيات إدارة المخاطر، فاعلية تنفيذها، وتحقيق أهداف التحول الرقمي، مع مراعاة الخصائص المحلية للبيئة الحكومية السعودية. كما توفر الدراسة قاعدة علمية للبحوث المستقبلية من خلال قياس أثر السياسات والإجراءات الوقائية على الحد من المخاطر السيبرانية، وتحليل العوامل التي تؤثر في فاعلية الاستراتيجيات المعتمدة، ما يسهم في إثراء الأدبيات المتعلقة بالأمن الرقمي، الحوكمة الإلكترونية، وإدارة المخاطر في المؤسسات العامة (Haque, 2020).

• الأهمية العملية

من الناحية العملية، تهدف الدراسة إلى تقديم توصيات تطبيقية تساعد الجهات الحكومية في المملكة على تعزيز فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني وتحسين قدرتها على مواجهة التهديدات الرقمية. فنتائج الدراسة توفر للجهات المسؤولة عن الأمن الرقمي إطاراً عملياً لتقييم الوضع الحالي، تحديد نقاط القوة والضعف في الاستراتيجيات المعتمدة، ووضع خطط تحسين مستمرة تتماشى مع متطلبات التحول الرقمي. كما تساعد الدراسة في رفع مستوى الوعي لدى صناع القرار حول أهمية حماية البيانات، ضمان استمرارية الخدمات الرقمية، وتقليل الخسائر الناتجة عن الهجمات الإلكترونية. وبذلك، تسهم الدراسة في تعزيز الثقة العامة في الخدمات الحكومية الرقمية، وتحسين كفاءة الأداء المؤسسي، فضلاً عن دعم الاستدامة الرقمية وتطوير بيئة أمن سيبراني قوية تواكب التطورات التكنولوجية العالمية مع مراعاة الخصوصية والقيم الوطنية (Johri, 2023).

أهداف الدراسة

الهدف الرئيسي

- تهدف الدراسة إلى تقييم فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية في ضوء التحول الرقمي، بما يسهم في تعزيز حماية البيانات، ضمان استمرارية الخدمات الرقمية، وتحقيق الاستفادة القصوى من التحول الرقمي في القطاع الحكومي.

الأهداف الفرعية

١. تحديد الاستراتيجيات المعتمدة لإدارة مخاطر الأمن السيبراني في الجهات الحكومية السعودية.
٢. تقييم مدى فاعلية تطبيق هذه الاستراتيجيات في حماية البيانات والمعلومات الحساسة.
٣. تحليل العلاقة بين جودة استراتيجيات إدارة المخاطر والأداء الرقمي للخدمات الحكومية.
٤. تحديد المعوقات التي تواجه الجهات الحكومية في تنفيذ استراتيجيات الأمن السيبراني.
٥. تقديم توصيات عملية لتعزيز فاعلية إدارة المخاطر السيبرانية وتحسين قدرة الجهات الحكومية على مواجهة التهديدات الرقمية.

تساؤلات الدراسة

الهدف الرئيسي

- تهدف الدراسة إلى تقييم فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية في ضوء التحول الرقمي، بما يسهم في تعزيز حماية البيانات، ضمان استمرارية الخدمات الرقمية، وتحقيق الاستفادة القصوى من التحول الرقمي في القطاع الحكومي.

الأهداف الفرعية

١. تحديد الاستراتيجيات المعتمدة لإدارة مخاطر الأمن السيبراني في الجهات الحكومية السعودية.
٢. تقييم مدى فاعلية تطبيق هذه الاستراتيجيات في حماية البيانات والمعلومات الحساسة.
٣. تحليل العلاقة بين جودة استراتيجيات إدارة المخاطر والأداء الرقمي للخدمات الحكومية.
٤. تحديد المعوقات التي تواجه الجهات الحكومية في تنفيذ استراتيجيات الأمن السيبراني.

٥. تقديم توصيات عملية لتعزيز فاعلية إدارة المخاطر السيبرانية وتحسين قدرة الجهات الحكومية على مواجهة التهديدات الرقمية.

فرضيات الدراسة

الفرضية الرئيسية

- استراتيجيات إدارة مخاطر الأمن السيبراني المطبقة في الجهات الحكومية بالمملكة العربية السعودية تؤثر بشكل إيجابي وذو دلالة إحصائية على فاعلية حماية البيانات وضمان استمرارية الخدمات الرقمية في ضوء التحول الرقمي.

الفرضيات الفرعية

١. هناك علاقة إيجابية بين وضوح الاستراتيجيات المعتمدة لإدارة المخاطر السيبرانية وفاعلية حماية البيانات.
٢. استخدام الإجراءات التقنية والإدارية الحديثة في إدارة المخاطر يعزز قدرة الجهات الحكومية على الاستجابة للتهديدات الرقمية.
٣. التدريب والتوعية المستمرة للعاملين في الأمن السيبراني يزيد من فاعلية تنفيذ الاستراتيجيات المتبعة.
٤. المعوقات التنظيمية والتقنية تؤثر سلبًا على فاعلية استراتيجيات إدارة المخاطر السيبرانية.
٥. تطبيق استراتيجيات متكاملة ومرنة لإدارة المخاطر يساهم في تحسين الأداء الرقمي وتحقيق أهداف التحول الرقمي في الجهات الحكومية.

النظرية العلمية المتبعة لإعداد البحث

اعتمدت الدراسة الحالية على نظرية إدارة المخاطر المؤسسية (Enterprise Risk Management Theory - ERM) بوصفها الإطار النظري الرئيس لتفسير فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية في ضوء التحول الرقمي. وتعد هذه النظرية من أكثر النظريات شمولاً في مجال إدارة المخاطر، إذ تنظر إلى المخاطر باعتبارها جزءاً لا يتجزأ من البيئة المؤسسية، وتتطلب إدارة استراتيجية متكاملة ترتبط بأهداف المؤسسة وعملياتها ومواردها وقراراتها. ومع تزايد الاعتماد على التقنيات الرقمية والأنظمة الإلكترونية في الجهات الحكومية السعودية، أصبحت المخاطر السيبرانية من أكثر

المخاطر تأثيراً في استمرارية الأعمال وجودة الخدمات الحكومية، الأمر الذي يجعل تطبيق مبادئ إدارة المخاطر المؤسسية ضرورة استراتيجية وليست مجرد إجراء تقني.

وتقوم نظرية إدارة المخاطر المؤسسية على افتراض رئيس يتمثل في أن المؤسسات التي تمتلك منظومة متكاملة لتحديد المخاطر وتحليلها وتقييمها والاستجابة لها تكون أكثر قدرة على تحقيق أهدافها وتقليل آثار التهديدات المحتملة. ولا تقتصر هذه المنظومة على الجوانب التقنية، بل تشمل أيضاً الجوانب الإدارية والتنظيمية والتشريعية والموارد البشرية، بحيث تصبح إدارة المخاطر جزءاً من ثقافة المؤسسة وأليات اتخاذ القرار فيها. وفي سياق الأمن السيبراني، تعني هذه الرؤية أن نجاح الجهة الحكومية في حماية أصولها الرقمية لا يعتمد فقط على استخدام تقنيات الحماية، وإنما يرتبط بوجود استراتيجية شاملة تتضمن الحوكمة، والسياسات، وإدارة المخاطر، والتوعية، والاستجابة للحوادث، والتحسين المستمر.

وتؤكد النظرية أن عملية إدارة المخاطر تمر بمجموعة من المراحل المترابطة تبدأ بتحديد مصادر المخاطر والتهديدات المحتملة، ثم تحليل احتمالية حدوثها وحجم تأثيرها، يلي ذلك تقييم أولوياتها واختيار وسائل المعالجة المناسبة، ثم متابعة تنفيذ الإجراءات الوقائية والرقابية، وأخيراً المراجعة المستمرة للتأكد من فاعلية الاستراتيجيات المطبقة. ويُعد هذا التسلسل المنهجي مناسباً لدراسة الأمن السيبراني في الجهات الحكومية، حيث تتغير طبيعة التهديدات الإلكترونية بصورة مستمرة نتيجة التطور التقني وظهور أساليب جديدة للهجمات السيبرانية، مما يتطلب مراجعة دورية للاستراتيجيات الأمنية وتحديثها بما يتلاءم مع طبيعة المخاطر المستجدة.

وفي ظل التحول الرقمي الذي تشهده المملكة العربية السعودية، توسعت الجهات الحكومية في استخدام الحوسبة السحابية، والذكاء الاصطناعي، وإنترنت الأشياء، والبيانات الضخمة، والخدمات الحكومية الرقمية، وهو ما أدى إلى زيادة حجم البيانات المتداولة وتنوع الأنظمة الرقمية المستخدمة. ورغم ما يوفره هذا التحول من مزايا كبيرة في تحسين جودة الخدمات الحكومية ورفع كفاءة الأداء، فإنه في الوقت نفسه يرفع من مستوى التعرض للمخاطر السيبرانية، مثل الاختراقات الإلكترونية، وسرقة البيانات، وهجمات الفدية، وتعطيل الخدمات الرقمية، وانتهاك خصوصية المعلومات. ومن هنا تبرز أهمية نظرية إدارة المخاطر المؤسسية، التي تؤكد ضرورة دمج إدارة المخاطر ضمن جميع مراحل التحول الرقمي، بحيث تصبح حماية المعلومات عنصراً أساسياً في تصميم وتنفيذ وتشغيل الأنظمة الرقمية.

كما تركز النظرية على مفهوم الشهية للمخاطر (Risk Appetite)، والذي يشير إلى المستوى المقبول من المخاطر الذي تستطيع المؤسسة تحمله في سبيل تحقيق أهدافها. وفي الجهات الحكومية، يُعد تحديد شهية المخاطر من العناصر المهمة عند تصميم

استراتيجيات الأمن السيبراني. إذ يساعد في تحديد أولويات الاستثمار في الضوابط الأمنية، وتوزيع الموارد، واتخاذ القرارات المتعلقة بإدارة التهديدات الرقمية. كما يسهم في تحقيق التوازن بين متطلبات الابتكار الرقمي من جهة، ومتطلبات حماية البيانات واستمرارية الخدمات الحكومية من جهة أخرى، بما يضمن تحقيق الكفاءة دون الإخلال بمستويات الأمن المطلوبة.

وتوضح النظرية كذلك أن فاعلية إدارة المخاطر تعتمد على تكامل الأدوار والمسؤوليات بين مختلف المستويات الإدارية داخل المؤسسة. بدءًا من الإدارة العليا التي تتولى رسم السياسات واعتماد الاستراتيجيات، مرورًا بالإدارات التنفيذية التي تطبق الضوابط والإجراءات، وانتهاءً بجميع الموظفين الذين يمثلون خط الدفاع الأول ضد المخاطر السيبرانية من خلال الالتزام بالإجراءات الأمنية والممارسات السليمة. وبمعنى ذلك أن نجاح استراتيجيات الأمن السيبراني لا يتحقق بالحلول التقنية وحدها، وإنما يتطلب وجود ثقافة تنظيمية داعمة للأمن السيبراني، وبرامج تدريب وتوعية مستمرة، وآليات فعالة للإبلاغ عن الحوادث والاستجابة لها.

وتنسجم هذه النظرية مع طبيعة الدراسة الحالية، حيث تُعد استراتيجيات إدارة مخاطر الأمن السيبراني المتغير المستقل، بينما تمثل فاعلية الأداء الأمني في الجهات الحكومية في ظل التحول الرقمي أو مستوى نجاح تطبيق تلك الاستراتيجيات المتغير الذي تسعى الدراسة إلى تفسيره. ومن خلال هذا الإطار النظري يمكن تفسير كيفية إسهام الاستراتيجيات الأمنية، مثل تحديد المخاطر، والتقييم المستمر، والرقابة، وإدارة الاستجابة للحوادث، والتوعية الأمنية، في تعزيز قدرة الجهات الحكومية على حماية أصولها الرقمية وتحقيق استدامة خدماتها الإلكترونية.

كما تتوافق نظرية إدارة المخاطر المؤسسية مع الأطر والمعايير الدولية في مجال الأمن السيبراني، مثل إطار NIST Cybersecurity Framework، ومعيار ISO/IEC 27001، وإطار COSO Enterprise Risk Management، والتي تؤكد جميعها أهمية تبني منهج استراتيجي متكامل لإدارة المخاطر، وربطها بالحوكمة المؤسسية، والتحسين المستمر، وإدارة الأداء، وهذا التوافق يعزز من ملاءمة النظرية لتفسير واقع الأمن السيبراني في الجهات الحكومية السعودية. التي تتبنى العديد من المعايير الوطنية والدولية ضمن برامج التحول الرقمي ورؤية المملكة العربية السعودية ٢٠٣٠.

وفي ضوء ما سبق، تُعد نظرية إدارة المخاطر المؤسسية إطارًا علميًا مثيرًا للدراسة الحالية، إذ تفسر بصورة منهجية العلاقة بين استراتيجيات إدارة مخاطر الأمن السيبراني وقدرة الجهات الحكومية على مواجهة التهديدات الرقمية في بيئة تنسم بالتغير المستمر. كما توفر أساسًا علميًا لتحليل النتائج المتوقعة للدراسة، والتي يُنتظر أن تشير إلى أن الجهات الحكومية التي تتبنى استراتيجيات متكاملة لإدارة مخاطر الأمن السيبراني، وتدمجها ضمن عملياتها الإدارية والتحول الرقمي، تحقق مستويات أعلى

من حماية المعلومات، واستمرارية الأعمال، وجودة الخدمات الرقمية، وتعزيز ثقة المستخدمين، بما يدعم تحقيق مستهدفات رؤية المملكة العربية السعودية ٢٠٣٠ في بناء حكومة رقمية آمنة وفعالة.

الفصل الثاني

الدراسات السابقة

يشكل الفصل الثاني الركيزة العلمية التي تستند إليها الدراسة، إذ يمثل الإطار الفكري الذي يُبنى عليه البحث من خلال تقديم عرض علمي متكامل للأدبيات ذات الصلة بموضوع الدراسة، وتحليل المفاهيم الرئيسية والاتجاهات الحديثة المرتبطة بإدارة مخاطر الأمن السيبراني في الجهات الحكومية في ظل التحول الرقمي. ويهدف هذا الفصل إلى بناء قاعدة معرفية متماسكة تساعد على فهم طبيعة المشكلة البحثية وأبعادها المختلفة، وتوضيح التطورات التي شهدتها مجال الأمن السيبراني على المستويين النظري والتطبيقي، مع التركيز على البيئة الحكومية السعودية التي تشهد تحولاً رقمياً متسارعاً وفق مستهدفات رؤية المملكة العربية السعودية ٢٠٣٠. كما يسهم الفصل في توضيح الأسس العلمية التي استند إليها الباحث عند صياغة الدراسة، بما يعزز من قوة البناء العلمي ويمنح القارئ تصوراً واضحاً عن الخلفية الفكرية التي انطلقت منها الدراسة.

ويتناول هذا الفصل بصورة منهجية المفاهيم الحديثة التي تشكل الأساس العلمي للدراسة، مع استعراض وتحليل الإنتاج العلمي السابق في مجال الأمن السيبراني وإدارة مخاطره، وإبراز أبرز الاتجاهات البحثية والنماذج العلمية التي تناولت هذا الموضوع. ولا يقتصر دور الفصل على عرض المعرفة النظرية، بل يمتد إلى تحليلها بصورة نقدية، وبيان أوجه الاتفاق والاختلاف بين نتائج الدراسات السابقة، والكشف عن الجوانب التي ما زالت بحاجة إلى المزيد من البحث والدراسة، الأمر الذي يبرز القيمة العلمية للدراسة الحالية. كما يسهم في بناء نموذج علمي متكامل يربط بين الجوانب النظرية والواقع العملي داخل الجهات الحكومية، ويوفر أساساً منطقياً لتفسير العلاقات التي سيتم اختبارها في الجانب التطبيقي.

وتنبع أهمية هذا الفصل من كونه يمثل المرجعية العلمية التي يعتمد عليها الباحث في تفسير النتائج التي سيتم التوصل إليها لاحقاً، إذ إن قوة أي دراسة علمية ترتبط بمدى متانة الأساس النظري الذي تستند إليه. كما يساعد هذا الفصل على توضيح التطورات التي شهدتها الأمن السيبراني في ظل التحول الرقمي، ويبرز أهمية تبني استراتيجيات متقدمة لإدارة المخاطر بما يضمن حماية الأصول الرقمية واستمرارية الخدمات الحكومية. ويُعد هذا الفصل أيضاً حلقة الوصل بين المعرفة الأكاديمية والتطبيق العملي، حيث يمهّد الطريق للفصول اللاحقة من خلال بناء إطار علمي متكامل يدعم تفسير النتائج واستخلاص الاستنتاجات بصورة دقيقة وموضوعية.

المتغير التابع والمستقل

تستند الدراسة الحالية إلى نموذج بحثي يهدف إلى قياس فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية في ضوء التحول الرقمي، وذلك من خلال دراسة تأثير مجموعة من المتغيرات المستقلة التي تمثل أهم الركائز اللازمة لتعزيز الأمن السيبراني في المؤسسات الحكومية، وقياس مدى انعكاسها على المتغير التابع المتمثل في فعالية إدارة مخاطر الأمن السيبراني في الجهات الحكومية. وقد تم اختيار هذه المتغيرات استناداً إلى الأدبيات العلمية الحديثة، والأطر الدولية لإدارة مخاطر الأمن السيبراني مثل إطار NIST Cybersecurity Framework، ومعيار ISO/IEC 27001، إضافة إلى التوجهات الوطنية للمملكة العربية السعودية في مجال الأمن السيبراني والتحول الرقمي.

أولاً: المتغير التابع: فعالية إدارة مخاطر الأمن السيبراني في الجهات الحكومية

تمثل فعالية إدارة مخاطر الأمن السيبراني في الجهات الحكومية المخرجات النهائية التي تسعى الدراسة إلى قياسها، ويقصد بها مدى قدرة الجهة الحكومية على التعرف على المخاطر السيبرانية وتحليلها وتقييمها والتعامل معها بصورة استباقية، بما يضمن حماية المعلومات والأصول الرقمية واستمرارية الخدمات الحكومية الإلكترونية. كما تعكس الفعالية قدرة المؤسسة على تقليل احتمالية وقوع الهجمات الإلكترونية، والحد من أثارها عند حدوثها، مع المحافظة على سرية المعلومات وسلامتها وإتاحتها، وهي المبادئ الأساسية للأمن السيبراني.

وتعد فعالية إدارة المخاطر السيبرانية من أهم مؤشرات نجاح المؤسسات الحكومية في ظل التحول الرقمي، حيث أصبحت الخدمات الحكومية تعتمد بصورة متزايدة على الأنظمة الرقمية، والحوسبة السحابية، وقواعد البيانات الضخمة، والذكاء الاصطناعي، مما أدى إلى اتساع نطاق التهديدات السيبرانية وتزايد تعقيدها. ولذلك فإن قدرة الجهات الحكومية على إدارة هذه المخاطر بصورة فعالة أصبحت عاملاً رئيساً في تحقيق الاستقرار المؤسسي وضمان استمرارية تقديم الخدمات للمواطنين والمستفيدين دون انقطاع.

كما ترتبط فعالية إدارة مخاطر الأمن السيبراني بمدى نجاح المؤسسة في تطبيق الضوابط الأمنية، والاستجابة السريعة للحوادث السيبرانية، وإدارة الأزمات الرقمية، ومراقبة التهديدات بصورة مستمرة، إضافة إلى قدرتها على التكيف مع التغيرات المتسارعة في بيئة المخاطر الإلكترونية. فكلما ارتفع مستوى الفعالية، زادت قدرة الجهة الحكومية على حماية بياناتها وتقليل الخسائر المحتملة وتعزيز ثقة المستفيدين في خدماتها الرقمية.

ومن المنظور الإداري، تمثل فعالية إدارة مخاطر الأمن السيبراني أحد المؤشرات الأساسية لقياس جودة الحوكمة الرقمية داخل الجهات الحكومية، إذ تعكس مدى تكامل السياسات والإجراءات والتقنيات والموارد البشرية في بناء منظومة أمنية متكاملة تدعم استدامة الأعمال وتحقيق الأهداف الاستراتيجية للجهة الحكومية.

ثانياً: المتغير المستقل الأول: تطبيق استراتيجيات إدارة مخاطر الأمن السيبراني

يقصد بتطبيق استراتيجيات إدارة مخاطر الأمن السيبراني مدى التزام الجهة الحكومية بتنفيذ السياسات والإجراءات والخطط التي تهدف إلى تحديد المخاطر السيبرانية وتقييمها ومعالجتها بصورة منهجية ومستدامة. ويشمل ذلك وضع السياسات الأمنية، وإجراء تقييمات دورية للمخاطر، وتصنيف الأصول الرقمية، وتحديد أولويات الحماية، وتطوير خطط الاستجابة للحوادث، ومتابعة تنفيذ الضوابط الأمنية وفق المعايير الوطنية والدولية.

وبعد هذا المتغير من أهم العوامل المؤثرة في نجاح إدارة المخاطر السيبرانية، لأن وجود استراتيجية واضحة يساهم في توحيد الجهود داخل المؤسسة، ويضمن التكامل بين الإدارات المختلفة في مواجهة التهديدات الرقمية. كما تساعد الاستراتيجيات الفعالة على تخمين سرعة اكتشاف المخاطر، وتقليل احتمالية وقوع الحوادث الأمنية، وتعزيز الجاهزية المؤسسية للتعامل مع الأزمات السيبرانية.

وفي ظل التحول الرقمي الذي تشهده الجهات الحكومية السعودية، أصبحت استراتيجيات إدارة المخاطر عنصراً أساسياً في جميع مراحل تصميم وتشغيل الأنظمة الرقمية. حيث تساهم في تحقيق التوازن بين متطلبات الابتكار الرقمي ومتطلبات حماية المعلومات، بما يضمن استمرارية الخدمات الحكومية وتحقيق أعلى مستويات الأمن الرقمي.

ثالثاً: المتغير المستقل الثاني: الجاهزية التقنية وبنية الأمن السيبراني

تشير الجاهزية التقنية وبنية الأمن السيبراني إلى مدى توافر البنية التحتية التقنية والأنظمة الأمنية التي تمكن الجهة الحكومية من حماية أصولها الرقمية والتصدي للتهديدات الإلكترونية بكفاءة. وتشمل هذه الجاهزية توفر مراكز البيانات الآمنة، وأنظمة الحماية المتقدمة، وجدران الحماية، وأنظمة كشف ومنع الاختراق، وإدارة الهوية والصلاحيات، وتقنيات التشفير، وأنظمة النسخ الاحتياطي، والحلول الخاصة بمراقبة الشبكات وإدارة الأحداث الأمنية.

وتكمن أهمية هذا المتغير في أن الاستراتيجيات الأمنية لا يمكن أن تحقق أهدافها دون وجود بنية تقنية قوية تدعم تنفيذها. فكلما كانت البنية التحتية أكثر تطوراً وتكاملاً، ارتفعت قدرة المؤسسة على اكتشاف التهديدات والاستجابة لها بصورة سريعة،

وتقليل الآثار السلبية للهجمات السيبرانية. كما تساعد الجاهزية التقنية على تعزيز استمرارية الأعمال وضمان توافر الخدمات الحكومية الرقمية حتى في حالات الطوارئ.

وفي البيئة الحكومية السعودية، أصبحت الجاهزية التقنية أحد المحاور الرئيسة للتحول الرقمي، حيث تستثمر الجهات الحكومية بصورة كبيرة في تطوير بنيتها الرقمية بما يتوافق مع متطلبات الهيئة الوطنية للأمن السيبراني وأفضل الممارسات العالمية، الأمر الذي يسهم في رفع كفاءة إدارة المخاطر وتعزيز حماية المعلومات الحكومية الحساسة.

رابعاً: المتغير المستقل الثالث: التوعية والتدريب في مجال الأمن السيبراني

يقصد بالتوعية والتدريب في مجال الأمن السيبراني جميع البرامج والأنشطة التي تستهدف رفع مستوى المعرفة والوعي الأمني لدى العاملين في الجهات الحكومية، وتنمية مهاراتهم في التعامل مع التهديدات السيبرانية والالتزام بالإجراءات والسياسات الأمنية. ويشمل ذلك الدورات التدريبية، وورش العمل، والمحاكاة العملية للهجمات الإلكترونية، وحملات التوعية المستمرة، والاختبارات الدورية لقياس مستوى الالتزام بالممارسات الأمنية.

وبعد العنصر البشري من أكثر عناصر الأمن السيبراني أهمية، حيث تشير العديد من الدراسات إلى أن نسبة كبيرة من الحوادث الأمنية تنتج عن أخطاء بشرية أو ضعف الوعي الأمني. ولذلك فإن الاستثمار في تدريب الموظفين يسهم في تقليل المخاطر الناتجة عن التصيد الإلكتروني، والهندسة الاجتماعية، وسوء استخدام الأنظمة، ويعزز من قدرة العاملين على اكتشاف التهديدات والإبلاغ عنها في الوقت المناسب.

كما تؤدي برامج التوعية إلى ترسيخ ثقافة الأمن السيبراني داخل الجهة الحكومية، بحيث تصبح حماية المعلومات مسؤولية مشتركة بين جميع العاملين، وليس مسؤولية الإدارات التقنية فقط. وبؤدي ذلك إلى رفع مستوى الالتزام بالسياسات الأمنية، وتحسين سرعة الاستجابة للحوادث، وتعزيز فعالية إدارة المخاطر على المستوى المؤسسي.

العلاقة بين المتغيرات المستقلة والمتغير التابع

تفترض الدراسة وجود علاقة تأثير إيجابية مباشرة بين المتغيرات المستقلة المتمثلة في تطبيق استراتيجيات إدارة مخاطر الأمن السيبراني، والجاهزية التقنية وبنية الأمن السيبراني، والتوعية والتدريب في مجال الأمن السيبراني وبين المتغير التابع فعالية إدارة مخاطر الأمن السيبراني في الجهات الحكومية.

فكلما ارتفع مستوى تطبيق الاستراتيجيات الأمنية وفق منهجية واضحة، وتوافرت بنية تقنية متقدمة تدعم عمليات الحماية والمراقبة والاستجابة، وازدادت برامج التوعية والتدريب التي تعزز كفاءة العنصر البشري، ارتفعت قدرة الجهات الحكومية على إدارة المخاطر السيبرانية بصورة أكثر كفاءة وفاعلية. وبؤدي هذا التكامل إلى تحسين عمليات اكتشاف التهديدات، وتسريع الاستجابة للحوادث، وتقليل احتمالات الاختراق، وحماية البيانات والأصول الرقمية، وضمان استمرارية الخدمات الحكومية.

وتستند هذه العلاقة إلى نظرية إدارة المخاطر المؤسسية (Enterprise Risk Management - ERM)، التي تؤكد أن إدارة المخاطر الفعالة تتحقق من خلال تكامل السياسات والإجراءات، والبنية التحتية، والعنصر البشري ضمن إطار مؤسسي موحد. وفي ضوء التحول الرقمي المتسارع في المملكة العربية السعودية، فإن تكامل هذه المتغيرات يمثل عاملاً أساسياً في تعزيز جاهزية الجهات الحكومية لمواجهة التهديدات السيبرانية، ورفع مستوى الأمن الرقمي، ودعم تحقيق مستهدفات رؤية المملكة العربية السعودية ٢٠٣٠ في بناء حكومة رقمية آمنة، مرنة، ومستدامة.

الدراسات السابقة

تزايد استخدام المؤسسات السعودية للتقنيات الرقمية. ورغم الجهود المبذولة للاستفادة من التحول الرقمي، إلا أن قلة من الشركات حققت نتائج ملموسة. وقد ربطت دراسات عديدة نجاح أو فشل عملية التحول الرقمي بالموظفين. وقد طرحت دراسة (Assiri, ٢٠٢٢) ثلاث فرضيات تتعلق بأمن التحول الرقمي، تشمل تحديد كيفية تطور الأمن نتيجة لتزايد استخدام الأنظمة الرقمية، بالإضافة إلى تحديد أفضل استراتيجيات إدارة المخاطر. وستلحق مجموعة من الجهات السعودية العامة والخاصة استبياناً إلكترونياً كجزء من هذه الدراسة. وخلصت الدراسة إلى أنه مع نمو التحول الرقمي، تزايد مخاطر الأمن، مما يستلزم تطبيق نظام أمني قوي وأكثر تدابير إدارة المخاطر فعالية. كما يجب على الشركات إشراك موظفيها في تطوير وتنفيذ التحول الرقمي للحفاظ على ولائهم. كذلك، يجب على جميع الموظفين فهم أهداف التحول الرقمي وغاياته وخططه والموافقة عليها. ويستطيع قادة الأعمال الناجحون بناء رؤية ملهمة، وتوحيد جهود الموظفين، وإشراكهم في تبني أساليب جديدة في العمل.

يُعد أمن المعلومات وخصوصيتها في الخدمات العامة من الاعتبارات الأساسية في عصرنا الرقمي، حيث تعتمد الحكومات بشكل متزايد على التكنولوجيا لتقديم الخدمات بكفاءة مع الحفاظ على سرية المعلومات الحساسة. ويعتمد نجاح استخدام هذه الخدمات الإلكترونية على مستوى ثقة المواطنين في قنوات الحكومة الإلكترونية. لذا، ينبغي أن يراعى تصميم مؤسسات الخدمة العامة سهولة استخدام ضوابط الأمان. في هذه الدراسة (Saeed, ٢٠٢٥)، نعرض نتائج دراسة كمية أجريت في المملكة العربية

السعودية لفهم تصورات المستخدمين النهائيين حول أمن المعلومات وخصوصيتها في استخدامهم للخدمات العامة. وبناءً على هذه النتائج، نقدم نموذجاً لتحسين جوانب أمن المعلومات وخصوصيتها، مما يُساعد صانعي السياسات والممارسين على تحسين تقديم الخدمات العامة إلكترونياً. ويمكن تطوير هذا النموذج في سياقات جغرافية مختلفة لتعزيز الأمن السيبراني في تقديم خدمات الحكومة الإلكترونية من خلال تضافر جهود المواطنين ومؤسسات تقديم الخدمات والهيئات الحكومية المعنية بالأمن السيبراني.

تتبنى المملكة العربية السعودية التحول الرقمي وخدمات الحكومة الإلكترونية، بهدف تحسين الكفاءة وسهولة الوصول والتركيز على المواطن. ومع ذلك، تواجه المملكة تحديات، منها التهديدات السيبرانية المتطورة. تهدف هذه الدراسة إلى بحث العوامل المؤثرة على ممارسات الأمن السيبراني لضمان موثوقية وأمن خدمات الحكومة الإلكترونية. تبحث دراسة (Al-Hawamleh, 2024) في الديناميكيات المتعددة الأوجه لممارسات الأمن السيبراني وتأثيرها على جودة وفعالية خدمات الحكومة الإلكترونية. تشمل العوامل الرئيسية التي تم استكشافها: الثقافة التنظيمية، والبنية التحتية التقنية، والالتزام بالمعايير واللوائح، وتدريب الموظفين وتوعيتهم، والاستثمار المالي في الأمن السيبراني. استخدمت هذه الدراسة المنهج الكمي لجمع البيانات من 320 مشاركاً. جمع الباحث 285 استبياناً مكتملاً، بعد استبعاد الإجابات غير الصالحة أو غير المكتملة، وحلل مجموعة البيانات النهائية باستخدام نمذجة المعادلات الهيكلية للمربعات الصغرى الجزئية. تُظهر النتائج أن الاستثمار المالي في الأمن السيبراني، وتدريب الموظفين، ورفع مستوى الوعي والالتزام بلوائح الأمن السيبراني، يؤثر بشكل كبير على تبني ممارسات فعالة في هذا المجال. مع ذلك، فإن العلاقة بين ثقافة المؤسسة وممارسات الأمن السيبراني ليست واضحة تماماً. يُثبت البحث وجود ارتباط إيجابي قوي بين ممارسات الأمن السيبراني وجودة خدمات الحكومة الإلكترونية، مُسلطاً الضوء على دور الأمن في تعزيز ثقة الجمهور ورضا المستخدمين. وتلبية الاحتياجات المتغيرة للمواطنين والشركات. يُساهم هذا البحث بأدلة تجريبية قيمة في مجال الحكومة الإلكترونية والأمن السيبراني، مُقدماً رؤى تُسهم في اتخاذ قرارات سياساتية قائمة على الأدلة، وتخصيص الموارد بشكل فعال. من خلال فهم الديناميكيات الدقيقة المؤثرة، تُصبح المملكة العربية السعودية في وضع أفضل لتعزيز بنيتها التحتية للحكومة الرقمية، وتوفير خدمات حكومية إلكترونية آمنة وعالية الجودة لمواطنيها.

حققت المملكة العربية السعودية إنجازات بارزة في مجال الأمن السيبراني. فقد حافظت على أليات تنظيمية متينة لمنع الجرائم الإلكترونية وتعقب مرتكبيها ومعاقبتهم، وذلك لحماية مصالح الأفراد والمؤسسات من مخاطر سرقة البيانات واختلاسها. ويعزز الاستخدام الواسع لتقنية المعلومات وخدماتها التدابير الأمنية. وتُعد التهديدات السيبرانية المتطورة باستمرار موضوعاً يثير

نقاشاً واسعاً. وفي هذا السياق، تُقدّم دراسة (Alhakami, ٢٠٢٤) نظرة شاملة على كيفية تطور الجرائم الإلكترونية في المملكة العربية السعودية حالياً، كما تُلقي نظرة على بعض أبرز الهجمات التي شهدتها المنطقة. ويهدف الإطار التشريعي والتدابير الحالية في المملكة إلى ردع النشاط الإجرامي عبر الإنترنت. وقد وُضعت نماذج كفاءة مختلفة لتلبية الكفاءات اللازمة في مجال مكافحة الجرائم الإلكترونية. ويمكن للباحثين المتخصصين في هذا المجال الاستفادة بشكل أكبر من خلال تطوير مستوى كفاءة متقدم لتحقيق أعلى مستويات الأمن. للإجابة على هذا السؤال البحثي، يستخدم هذا التقييم منهجية مختبر تجارب وتقييم اتخاذ القرارات الضبابية (Fuzzy-DMTAEI)، وعملية التحليل الهرمي الضبابية (F.AHP)، ومنهجية TOPSIS الضبابية لتحقيق تطوير الكفاءات القطاعية في سياسة الأمن السيبراني. كما يناقش أوجه التشابه والاختلاف بين هذه المنهجيات الثلاث. وقد أظهر تحليل الأمن السيبراني أن المركز الوطني للأمن السيبراني يحظى بأعلى أولوية. وتختتم الدراسة باستعراض التحديات التي لا تزال بحاجة إلى دراسة وحل لتفعيل آليات أمن إلكتروني أكثر متوقعة وفعالية، بما يُسهم في بناء اقتصاد أكثر قوة قائم على خدمات تكنولوجيا المعلومات في المملكة العربية السعودية. علاوة على ذلك، يحتاج متخصصو الأمن السيبراني وصناع السياسات إلى توحيد جهودهم لحماية الأصول الرقمية للبلاد في عصر الحرب السيبرانية العلنية والسرية.

يتمحور عصرنا الحالي حول تكنولوجيا المعلومات، إذ نشهد نهضة في مجال المعلومات وتوسعها على مستويات ومجالات متعددة. ويسعى المتخصصون في التكنولوجيا، ممن يمتلكون معرفة واسعة بها وشغفاً كبيراً بها، إلى نشر هذه المعلومات ومعالجتها على النحو الأمثل، وقد أصبحت الحواسيب اليوم من أهم الأدوات في العمليات الحكومية. وبدأت الشركات الكبرى بالفعل في استخدامها في معظم قطاعات أعمالها، وساهمت في توجيه بعض الإجراءات الحكومية نحو الحكومة الإلكترونية المشتركة، التي تتيح للمواطنين الوصول إلى الخدمات الحكومية من منازلهم عبر حواسيبهم. ومن الجدير بالذكر أنه مع ازدياد استخدام الحواسيب، ازدادت الجرائم الإلكترونية، مما ساهم في سنّ قوانين في مختلف الدول لمكافحتها. ومع تطور التكنولوجيا، تزايدت تعقيدات هذه التهديدات السيبرانية وتأثيرها، مما يشكل تحديات كبيرة للأمن السيبراني. يناقش دراسة (Alkhalifa, ٢٠٢٤) دور التكنولوجيا في مكافحة الجرائم السيبرانية، واللوائح المنظمة لها، والسلوكيات المسموح بها في استخدامها في المملكة العربية السعودية. كما يحلل البحث الجرائم السيبرانية في المملكة ونظام مكافحتها.

التعليق على الدراسات السابقة:

• أوجه التشابه في الدراسات السابقة

تتشترك الدراسات السابقة في التأكيد على الدور المحوري للأمن السيبراني في ضمان فاعلية التحول الرقمي داخل المؤسسات الحكومية والخاصة في المملكة العربية السعودية. فقد أظهرت جميع الدراسات أن نجاح التحول الرقمي يرتبط ارتباطاً وثيقاً بفاعلية استراتيجيات إدارة المخاطر السيبرانية، ومدى تكاملها مع السياسات الإدارية والبيئة التقنية. كما أكدت الدراسات على أهمية تدريب الموظفين وزيادة وعيهم بالأمن السيبراني، وإشراكهم في تبني الإجراءات الوقائية والتقنية الجديدة، بما يضمن استمرارية تقديم الخدمات الرقمية وحماية المعلومات الحساسة. وتشير الدراسات أيضاً إلى أن الاستثمار المالي في الأمن السيبراني، وتطوير البنية التحتية الرقمية، وتزام الجهات الحكومية بالمعايير واللوائح، يمثلون عوامل مؤثرة في تعزيز فاعلية ممارسات الأمن السيبراني وتحقيق الثقة لدى المستفيدين.

• أوجه الاختلاف في الدراسات السابقة

رغم التشابه في التركيز على الأمن السيبراني والتحول الرقمي، تختلف الدراسات في منهجية البحث والأبعاد التي تناولتها. فبعض الدراسات ركزت على تصورات المستخدمين النهائيين حول أمن المعلومات وخصوصيتها في الخدمات العامة، بينما تناولت دراسات أخرى العوامل التنظيمية والفنية التي تؤثر على جودة الخدمات الإلكترونية مثل الثقافة التنظيمية، والاستثمار المالي، والتدريب والتوعية. كما اختلفت الدراسات في نطاقها المكاني والزمني، فقد ركزت بعض الدراسات على عدد محدود من الجهات الحكومية أو الشركات الخاصة، في حين شملت أخرى جهات متعددة عبر مناطق مختلفة في المملكة. كما تنوعت أدوات البحث بين الاستبيانات الكمية، ونماذج المعادلات الهيكلية، والتقييمات التجريبية المعتمدة على تقنيات التحليل الضبابي، مما أدى إلى اختلاف نتائجها من حيث تحديد أولويات المخاطر وتقييم فاعلية الاستراتيجيات.

• الفجوات البحثية التي يميزها البحث الحالي

تشير مراجعة الدراسات السابقة إلى وجود عدة فجوات يمكن أن يعالجها البحث الحالي. أولاً، هناك نقص في الدراسات التي تربط بشكل مباشر بين فاعلية استراتيجيات إدارة المخاطر السيبرانية وأداء الجهات الحكومية الرقمية في سياق التحول الرقمي، مع مراعاة كافة الأبعاد البشرية، التقنية، والتنظيمية. ثانياً، معظم الدراسات ركزت على جانب واحد من الأمن السيبراني، مثل حماية البيانات أو تصورات المستخدمين، دون دراسة شاملة تتضمن استراتيجيات الوقاية والاستجابة والتعافي من التهديدات الرقمية. ثالثاً، هناك ندرة في الدراسات التي تقدم توصيات عملية قابلة للتطبيق لتعزيز قدرة الجهات الحكومية على مواجهة

المخاطر السيبرانية الحديثة في بيئة التحول الرقمي. أخيرًا، لم تتناول الدراسات السابقة بشكل كافٍ تقييم الفاعلية الشاملة للاستراتيجيات الحالية وقياس أثرها على استمرارية الخدمات الرقمية، وهو ما يمثل مساهمة جوهرية للبحث الحالي في سد هذه الفجوات وتقديم رؤية علمية وعملية متكاملة لدعم الأمن السيبراني في المملكة.

المنطلقات النظرية للدراسة

• مفهوم إدارة مخاطر الأمن السيبراني

تُعرف إدارة مخاطر الأمن السيبراني بأنها العملية المنهجية التي تهدف إلى التعرف على التهديدات السيبرانية، تقييم المخاطر المرتبطة بها، ووضع استراتيجيات وقائية وتصحيحية للحد من أثارها على المؤسسات. وتشمل هذه العملية مجموعة متكاملة من الإجراءات والسياسات التي تهدف إلى حماية المعلومات والأنظمة الرقمية من الهجمات الإلكترونية، الاختراقات، وسرقة البيانات، فضلاً عن التهديدات المرتبطة بالبنية التحتية الرقمية الحيوية. وتشير الدراسات النظرية إلى أن إدارة المخاطر السيبرانية ليست مجرد إجراءات تقنية، بل تشمل بعداً تنظيمياً وإدارياً يضمن التنسيق بين السياسات الأمنية، التقنيات المستخدمة، والتدريب المستمر للعاملين في المؤسسات، بما يعزز قدرة المؤسسة على التكيف مع التهديدات الرقمية المتغيرة باستمرار (Jalali, 2019).

• استراتيجيات إدارة المخاطر السيبرانية

تشمل الاستراتيجيات الفعالة لإدارة المخاطر السيبرانية مجموعة من الإجراءات المنهجية التي تركز على الوقاية، الكشف، الاستجابة، والتعافي من التهديدات. ومن بين هذه الاستراتيجيات: تطوير سياسات أمنية واضحة، استخدام ضوابط تقنية متقدمة، إجراء تقييم دوري للمخاطر، وتطبيق خطط استجابة للطوارئ. وتوضح الأدبيات النظرية أن الاستراتيجيات المرنة والقابلة للتطوير وفق التغيرات التقنية الحديثة تساهم بشكل كبير في تعزيز الفاعلية التشغيلية للجهات الحكومية، وتحافظ على سلامة البيانات والمعلومات الحيوية. كما أن دمج استراتيجيات الإدارة مع أهداف التحول الرقمي يساهم في تحقيق التوازن بين الابتكار التكنولوجي وحماية المعلومات، ويقلل من المخاطر التشغيلية المرتبطة بالنمو الرقمي في تقديم الخدمات الحكومية (Knowles, 2026).

• فاعلية استراتيجيات الأمن السيبراني

تشير الدراسات النظرية إلى أن فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني تعتمد على مدى تكاملها مع البنية التنظيمية والتقنية للجهة الحكومية، وجودة تنفيذها، وكفاءة الموارد البشرية المعنية. فكلما كانت الاستراتيجيات أكثر وضوحاً وتطبيقاً

بشكل متحج، زادت القدرة على الوقاية من الهجمات الإلكترونية والاستجابة السريعة لأي تهديد محتمل، ما ينعكس إيجاباً على استمرارية تقديم الخدمات الرقمية للمستفيدين. كما أن تقييم الفاعلية يشمل القدرة على حماية البيانات، الالتزام بالمعايير الوطنية والدولية للأمن السيبراني، وضمان استدامة العمليات الرقمية، مما يجعل تقييم هذه الفاعلية أمراً جوهرياً لفهم العلاقة بين إدارة المخاطر والأداء الرقمي (Nygard، ٢٠٢١).

• التحول الرقمي وعلاقته بإدارة المخاطر

يشير التحول الرقمي في الجهات الحكومية إلى استخدام التكنولوجيا الرقمية في تقديم الخدمات، تحسين الكفاءة التشغيلية، وتسهيل الوصول إلى المعلومات والخدمات للمستفيدين. ويبرز التحول الرقمي كعامل رئيسي يضاعف أهمية الأمن السيبراني، إذ أن زيادة الاعتماد على الأنظمة الرقمية تزيد من احتمالية التعرض للتهديدات السيبرانية. ومن هذا المنطلق، يجب أن تكون استراتيجيات إدارة المخاطر السيبرانية مصممة لتتكامل مع أهداف التحول الرقمي، بحيث توفر حماية مستمرة للبيانات والأنظمة، مع تمكين الجهات الحكومية من تحقيق الفاعلية التشغيلية، الابتكار في الخدمات، وتعزيز الثقة العامة في الأنظمة الرقمية الحكومية (Bennouk، ٢٠٢٤).

• التحديات النظرية والتطبيقية

تواجه الجهات الحكومية تحديات متعددة في إدارة المخاطر السيبرانية تشمل التغير السريع في طبيعة التهديدات الرقمية، قلة الموارد المتخصصة، ضعف الوعي الأمني بين الموظفين، وصعوبة دمج استراتيجيات الأمن مع أهداف التحول الرقمي. وتشير الدراسات النظرية إلى أن معالجة هذه التحديات تتطلب اعتماد استراتيجيات شاملة تشمل الجوانب التقنية والتنظيمية والبشرية، مع تقييم مستمر للتهديدات وتحديث السياسات والإجراءات الأمنية بما يتوافق مع المتطلبات المحلية والمعايير العالمية للأمن السيبراني. ويبرز من هذا السياق أن تطوير فاعلية استراتيجيات إدارة المخاطر ليس مجرد مسألة تقنية، بل يمثل عملية متكاملة تشمل التخطيط، التنفيذ، والمتابعة لضمان قدرة الجهات الحكومية على حماية البيانات واستمرارية الخدمات الرقمية بفاعلية (Slapničar، ٢٠٢٥).

الفصل الثالث

منهجية الدراسة

المقدمة

يمثل الفصل الثالث الجانب المنهجي للدراسة، ويُعد من أكثر الفصول أهمية لأنه يوضح الآليات العلمية والإجراءات المنظمة التي تتبعها الباحثة لتنفيذ الدراسة الميدانية بصورة تضمن الوصول إلى نتائج دقيقة وموثوقة. ويهدف هذا الفصل إلى توضيح الكيفية التي تم من خلالها تصميم الدراسة وتنفيذها وفق منهج علمي يتسم بالموضوعية والدقة، مع بيان الأسس التي اعتمد عليها الباحثة في اختيار الإجراءات المناسبة لطبيعة مشكلة الدراسة وأهدافها. كما يوضح هذا الفصل التسلسل المنطقي للخطوات البحثية منذ مرحلة التخطيط وحتى مرحلة تجهيز البيانات للتحليل، بما يعكس التزام الدراسة بالمعايير الأكاديمية المعتمدة في البحوث العلمية.

ويستعرض الفصل الإجراءات التطبيقية التي تم اتباعها لضمان الحصول على بيانات دقيقة تمثل الواقع الفعلي للجهات الحكومية محل الدراسة، مع توضيح الأسس العلمية التي استند إليها الباحثة في اختيار المشاركين وآليات الوصول إليهم، بالإضافة إلى الإجراءات التي اتخذت لضمان جودة البيانات وسلامتها. كما يتناول هذا الفصل الضوابط التي تحكم تنفيذ الدراسة، وآليات التحقق من موثوقية أدوات القياس، والإجراءات التي تكفل تحقيق الصدق والثبات، بما يساهم في تعزيز مصداقية النتائج التي سيتم التوصل إليها. ويعكس ذلك التزام الدراسة بالمنهجية العلمية التي تضمن إمكانية الاعتماد على نتائجها والاستفادة منها في تطوير الممارسات المتعلقة بإدارة مخاطر الأمن السيبراني.

وتبرز أهمية هذا الفصل في أنه يمثل الأساس الذي بُني عليه النتائج النهائية للدراسة، إذ إن دقة الإجراءات المنهجية تنعكس بصورة مباشرة على جودة البيانات وموضوعية التحليلات والاستنتاجات. كما يساهم في تعزيز الشفافية العلمية من خلال توضيح جميع الخطوات التي تتبعها الباحثة أثناء تنفيذ الدراسة، مما يمنح القارئ القدرة على تقييم مدى ملاءمة الإجراءات لطبيعة المشكلة البحثية، وبتحقيق إمكانية إعادة تطبيق الدراسة في بيئات مشابهة للتحقق من نتائجها أو مقارنتها بدراسات مستقبلية. وبذلك يشكل هذا الفصل حلقة أساسية تربط بين الإطار النظري والتطبيق الميداني، وتساهم في تحقيق أهداف الدراسة بصورة علمية ومنهجية.

مجتمع البحث

يتمثل مجتمع البحث في جميع العاملين والمسؤولين المعنيين بالأمن السيبراني، وإدارة المخاطر، وتقنية المعلومات، والتحول الرقمي، وإدارة الحوكمة والالتزام، والإدارات ذات العلاقة داخل الجهات الحكومية بالمملكة العربية السعودية. ويشمل ذلك القيادات الإدارية، ومديري إدارات الأمن السيبراني، وأخصائيي الأمن السيبراني، ومحليي المخاطر، ومهندسي الشبكات، ومشرفي الأنظمة، وموظفي تقنية المعلومات، بالإضافة إلى العاملين في الإدارات التي تتعامل بصورة مباشرة مع تطبيق السياسات الأمنية وإدارة المخاطر الرقمية. وقد تم اختيار هذا المجتمع لأنه يمثل الفئة الأكثر ارتباطاً بموضوع الدراسة، والأكثر قدرة على تقييم واقع استراتيجيات إدارة مخاطر الأمن السيبراني ومدى فاعليتها في ظل التحول الرقمي الذي تشهده الجهات الحكومية السعودية. ويستند اختيار مجتمع البحث إلى أن العاملين في هذه الجهات يمتلكون المعرفة والخبرة العملية المتعلقة بتطبيق السياسات الأمنية، وتنفيذ ضوابط الأمن السيبراني، وإدارة الحوادث الإلكترونية، ومتابعة الامتثال للأنظمة والتعليمات الصادرة عن الجهات التنظيمية المختصة، مثل الهيئة الوطنية للأمن السيبراني. كما أن طبيعة عملهم اليومية تجعلهم الأكثر قدرة على تقييم مستوى الجاهزية التقنية، ومدى كفاءة البنية التحتية الأمنية، وفاعلية برامج التوعية والتدريب، الأمر الذي يجعل بياناتهم أكثر دقة وموضوعية عند قياس متغيرات الدراسة.

ويتميز مجتمع الدراسة بالتنوع من حيث المستويات الوظيفية، والخبرات العملية، والتخصصات التقنية والإدارية، إضافة إلى اختلاف الجهات الحكومية التي ينتمي إليها المشاركون، وهو ما يساهم في الحصول على بيانات تمثل واقع الأمن السيبراني في القطاع الحكومي بصورة أكثر شمولاً. كما يسمح هذا التنوع بدراسة الاختلافات في وجهات النظر بين العاملين وفقاً لمتغيراتهم الوظيفية. الأمر الذي يثري نتائج الدراسة ويمنحها قدرة أكبر على تفسير العوامل المؤثرة في فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني.

كما يتوافق اختيار مجتمع البحث مع طبيعة المنهج الكمي، الذي يتطلب الحصول على بيانات من عدد مناسب من أفراد المجتمع باستخدام أداة قياس موحدة، بما يسمح بإجراء التحليلات الإحصائية واختبار العلاقات بين المتغيرات بصورة دقيقة. ويُعد الاعتماد على العاملين ذوي العلاقة المباشرة بالأمن السيبراني والتحول الرقمي عاملاً مهماً في تعزيز جودة البيانات، حيث تستند إجاباتهم إلى الخبرة العملية والمعرفة المهنية، وليس إلى الانطباعات العامة، مما يرفع من مستوى صدق النتائج وإمكانية الاعتماد عليها عند صياغة التوصيات.

وتكتسب دراسة هذا المجتمع أهمية خاصة في ظل التوسع الكبير الذي تشهده المملكة العربية السعودية في مجال الحكومة الرقمية، حيث أصبحت الجهات الحكومية تعتمد بصورة متزايدة على الأنظمة الإلكترونية والخدمات الرقمية، وهو ما يتطلب تطوير استراتيجيات متقدمة لإدارة مخاطر الأمن السيبراني وضمان استمرارية الخدمات وحماية البيانات الحكومية. ولذلك فإن دراسة هذا المجتمع تسهم في تقديم مؤشرات علمية يمكن الاستفادة منها في تطوير السياسات الأمنية، ورفع مستوى الجاهزية المؤسسية، وتعزيز كفاءة إدارة المخاطر بما يتوافق مع مستهدفات رؤية المملكة العربية السعودية ٢٠٣٠.

المنهجية وطرق البحث

تعتمد هذه الدراسة على المنهجية الكمية كخيار رئيسي لدراسة فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية. وتتميز المنهجية الكمية بقدرتها على قياس المتغيرات بدقة وتحليل العلاقات بينها بأسلوب إحصائي موضوعي، ما يجعلها الأنسب لدراسة العلاقة بين سياسات واستراتيجيات الأمن السيبراني وفعاليتها في حماية البيانات وضمان استمرارية تقديم الخدمات الرقمية. كما أن المنهج الكمي يمكن الباحث من اختبار الفرضيات العلمية التي تم صياغتها استناداً إلى الإطار النظري، مما يوفر نتائج قابلة للتعميم وتعزز موثوقية الاستنتاجات.

• تصميم البحث

تم تبني التصميم الوصفي-العلاقاتي للدراسة، إذ يسعى البحث أولاً إلى وصف الوضع الحالي لاستراتيجيات إدارة المخاطر السيبرانية في الجهات الحكومية، مع تحليل العناصر الأساسية لهذه الاستراتيجيات من حيث شموليتها وفعاليتها. كما يركز الجانب العلاقاتي على تحديد العلاقة بين تطبيق الاستراتيجيات وفعاليتها في حماية البيانات واستمرارية الخدمات الرقمية، إضافة إلى قياس أثر هذه الاستراتيجيات على أداء التحول الرقمي. ويساعد هذا التصميم على توضيح نقاط القوة والضعف في الاستراتيجيات الحالية، وتحليل مدى كفاءتها في مواجهة التهديدات السيبرانية الحديثة، بما يتيح تقديم توصيات علمية وعملية دقيقة.

• مجتمع وعينة البحث

يشمل مجتمع الدراسة جميع الجهات الحكومية السعودية التي تعتمد على الأنظمة والخدمات الرقمية في تقديم خدماتها للمواطنين والمستفيدين. ولضمان دقة البيانات، تم اختيار عينة ممثلة من المسؤولين التنفيذيين والإداريين والفنيين المكلفين بإدارة الأمن السيبراني في هذه الجهات، باعتبارهم الأطراف الأكثر معرفة بتطبيق الاستراتيجيات وفعاليتها. كما تم اعتماد العينة

العشوائية التطبيقية لتوزيع المستجيبين بحسب مستوى الوظائف ومسؤولياتهم، بما يضمن تمثيل جميع الفئات ذات العلاقة ويعكس الصورة الحقيقية للوضع الأمني السيبراني في الجهات الحكومية المختلفة.

• أدوات جمع البيانات

تم اعتماد الاستبيان الكمي المهيكل والمغلق كأداة رئيسية لجمع البيانات، حيث صُمم ليغطي جميع أبعاد الدراسة، بما يشمل الاستراتيجيات المعتمدة لإدارة المخاطر، فاعليتها في حماية البيانات، مستوى الالتزام بالإجراءات الأمنية، وتحديات التنفيذ. وتم استخدام مقياس ليكرت الخماسي لقياس درجة الاتفاق أو الاختلاف مع كل بيان، مما يسهل تحويل البيانات النوعية إلى بيانات كمية قابلة للتحليل الإحصائي. وقد تم اختيار الاستبيان على عينة تجريبية أولية للتأكد من وضوح الأسئلة وملاءمتها، كما تم تقييم موثوقيته باستخدام معامل كرونباخ ألفا لضمان اتساق الإجابات وثباتها.

• أساليب تحليل البيانات

بعد جمع الاستبيانات، تم استخدام مجموعة من الأساليب الإحصائية لتحليل البيانات. شملت هذه الأساليب الإحصاءات الوصفية لتحديد الخصائص الأساسية للمتغيرات، والتحليل الارتباطي لقياس العلاقة بين استراتيجيات إدارة المخاطر وفعاليتها، بالإضافة إلى التحليل الانحداري لتحديد مدى تأثير هذه الاستراتيجيات على حماية البيانات واستمرارية الخدمات الرقمية. كما تم اختيار الفرضيات الفرعية والرئيسية باستخدام الاختبارات الإحصائية المناسبة، مما يضمن موثوقية النتائج ويتيح استخلاص استنتاجات دقيقة تدعم تقديم توصيات عملية للجهات الحكومية.

تعكس هذه المنهجية الكمية الممنهجة قدرة الدراسة على تقديم تحليل علمي شامل لفاعلية استراتيجيات إدارة مخاطر الأمن السيبراني، وتتيح استكشاف العلاقة بين هذه الاستراتيجيات والأداء الرقمي للجهات الحكومية، بما يسهم في تعزيز أمن المعلومات، استدامة الخدمات الرقمية، وتحقيق أهداف التحول الرقمي في المملكة.

خطوات جمع البيانات

اتبعت الدراسة الحالية المنهجية الكمية باعتبارها المنهج الأكثر ملاءمة لتحقيق أهدافها، حيث تعتمد هذه المنهجية على جمع البيانات الرقمية من أفراد مجتمع الدراسة وتحليلها باستخدام الأساليب الإحصائية المناسبة لاختبار الفرضيات وقياس

العلاقات بين المتغيرات. وتم تنفيذ عملية جمع البيانات وفق مجموعة من الخطوات العلمية المتسلسلة التي تضمن الحصول على بيانات دقيقة وموثوقة يمكن الاعتماد عليها في تفسير نتائج الدراسة والوصول إلى استنتاجات موضوعية.

١. تحديد البيانات المطلوبة

بدأت عملية جمع البيانات بتحديد نوعية المعلومات اللازمة للإجابة عن أسئلة الدراسة وتحقيق أهدافها، وذلك في ضوء الإطار النظري والدراسات السابقة المتعلقة بالأمن السيبراني وإدارة المخاطر والتحول الرقمي. وتم تحديد البيانات التي تقيس مستوى تطبيق استراتيجيات إدارة مخاطر الأمن السيبراني، ومدى توافر الجاهزية التقنية وبنية الأمن السيبراني، ومستوى التوعية والتدريب الأمني، إضافة إلى البيانات التي تعكس مستوى فعالية إدارة مخاطر الأمن السيبراني داخل الجهات الحكومية. كما شملت البيانات بعض الخصائص الديموغرافية والوظيفية للمشاركين، بما يساهم في وصف عينة الدراسة وتحليل نتائجها بصورة أكثر دقة.

٢. تصميم أداة الدراسة

اعتمدت الدراسة على الاستبانة بوصفها الأداة الرئيسة لجمع البيانات، نظرًا لملاءمتها للدراسات الكمية، وقدرتها على جمع عدد كبير من الاستجابات خلال فترة زمنية مناسبة، مع تحقيق مستوى مرتفع من التوحيد في طريقة القياس. وقد صُممت الاستبانة بالاستناد إلى الأدبيات العلمية، والدراسات السابقة، والأطر والمعايير الدولية ذات العلاقة بالأمن السيبراني، مع مراعاة أن تغطي جميع أبعاد الدراسة بصورة شاملة.

كما صيغت عبارات الاستبانة بلغة واضحة ودقيقة تتناسب مع طبيعة أفراد مجتمع الدراسة، واعتمدت على مقياس ليكرت الخماسي الذي يتيح للمشاركين التعبير عن درجة موافقتهم على العبارات، بدءًا من (أوافق بشدة) وحتى (لا أوافق بشدة). ويُعد هذا المقياس من أكثر المقاييس استخدامًا في الدراسات الإدارية والتقنية، لما يوفره من سهولة في التطبيق وإمكانية إخضاع نتائجه للتحليل الإحصائي.

٣. التحقق من صدق وثبات أداة الدراسة

بعد الانتهاء من إعداد الاستبانة، تم إخضاعها لعمليات التحقق من الصدق والثبات لضمان صلاحيتها للاستخدام الميداني. وقد تم عرضها على مجموعة من المحكمين من ذوي الخبرة في مجالات الأمن السيبراني، وتقنية المعلومات، وإدارة المخاطر، والبحث العلمي، بهدف التأكد من سلامة الصياغة ووضوح العبارات ومدى ارتباطها بأهداف الدراسة.

كما تم إجراء الاختبارات الإحصائية اللازمة للتحقق من ثبات الأداة، بما يضمن اتساق إجابات المشاركين وإمكانية الاعتماد على النتائج المستخلصة منها. وتعد هذه المرحلة من أهم مراحل الدراسات الكمية، لأنها تعزز موثوقية البيانات، وتحد من احتمالية الخطأ في القياس، وتزيد من دقة النتائج النهائية.

٤. توزيع الاستبانة على أفراد العينة

بعد التأكد من صلاحية أداة الدراسة، تم توزيع الاستبانة على أفراد العينة المستهدفة باستخدام الوسائل الإلكترونية المناسبة، مثل منصات الاستبيانات الإلكترونية، والبريد الإلكتروني المؤسسي، وروابط الاستبانة الرقمية، بما يتناسب مع طبيعة البيئة الحكومية التي تعتمد بصورة كبيرة على الوسائل الرقمية في التواصل الداخلي.

وقد روعي أثناء عملية التوزيع توضيح الهدف العلمي للدراسة للمشاركين، والتأكيد على أن المشاركة اختيارية، وأن جميع البيانات ستستخدم لأغراض البحث العلمي فقط، مع الالتزام التام بسرية المعلومات وعدم الإفصاح عن أي بيانات شخصية أو وظيفية يمكن أن تؤدي إلى التعرف على هوية المشاركين. وأسهم ذلك في تعزيز ثقة أفراد العينة وتشجيعهم على تقديم إجابات دقيقة وصادقة.

٥. مراجعة الاستبانات وتجهيز البيانات

بعد انتهاء فترة جمع البيانات، تمت مراجعة جميع الاستبانات المستلمة للتأكد من اكتمال الإجابات وخلوها من البيانات الناقصة أو غير المنطقية. كما تم استبعاد الاستبانات التي لا تستوفي شروط التحليل الإحصائي. ثم جرى ترميز الإجابات وتحويلها إلى بيانات رقمية وإدخالها إلى أحد البرامج الإحصائية المتخصصة، تمهيداً لإجراء عمليات التحليل الوصفي والاستدلالي.

وتعد هذه المرحلة من المراحل الجوهرية في المنهجية الكمية، إذ إن جودة مراجعة البيانات وترميزها تؤثر بصورة مباشرة في دقة التحليلات الإحصائية، وتحد من احتمالية وقوع الأخطاء أثناء المعالجة الإحصائية.

٦. إعداد البيانات للتحليل الإحصائي

في المرحلة الأخيرة، تم تنظيم البيانات في قاعدة بيانات إلكترونية، وإجراء مراجعة إحصائية أولية للتأكد من جاهزيتها للتحليل، وذلك من خلال التحقق من عدم وجود قيم مفقودة أو متطرفة قد تؤثر في النتائج. وبعد ذلك تم تجهيز البيانات لإجراء التحليلات الإحصائية المناسبة، مثل الإحصاءات الوصفية، وتحليل الارتباط، وتحليل الانحدار، واختبار الفرضيات، بما يسمح بقياس أثر

تطبيق استراتيجيات إدارة مخاطر الأمن السيبراني، والجاهزية التقنية وبنية الأمن السيبراني، والتوعية والتدريب في مجال الأمن السيبراني في فعالية إدارة مخاطر الأمن السيبراني في الجهات الحكومية.

وقد أسهم اتباع هذه الخطوات المنهجية المتسلسلة في توفير بيانات دقيقة وموثوقة تعكس واقع الجهات الحكومية السعودية، الأمر الذي يدعم الوصول إلى نتائج علمية يمكن الاستفادة منها في تطوير استراتيجيات إدارة مخاطر الأمن السيبراني، وتعزيز جاهزية الجهات الحكومية لمواجهة التهديدات الرقمية، ودعم مسيرة التحول الرقمي وتحقيق مستهدفات رؤية المملكة العربية السعودية ٢٠٣٠.

أدوات الدراسة

تمثل أدوات الدراسة الركيزة الأساسية لجمع المعلومات وتحليلها في ضوء المنهجية الكمية المعتمدة في هذا البحث، إذ تهدف إلى توفير بيانات دقيقة وقابلة للتحليل الإحصائي حول فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية. واعتمدت الدراسة على الاستبيان الكمي المهيكل والمغلق كأداة رئيسية لجمع البيانات، نظرًا لقدرته على قياس المتغيرات بطريقة منظمة وموضوعية، وتحويل الآراء والملاحظات إلى بيانات رقمية قابلة للتحليل.

صُمم الاستبيان ليغطي جميع أبعاد الدراسة، بدءًا من السياسات والاستراتيجيات المعتمدة لإدارة المخاطر السيبرانية، ومرورًا بفاعلية تنفيذ هذه الاستراتيجيات في حماية البيانات وضمان استمرارية الخدمات الرقمية، وصولًا إلى التحديات والمعوقات التي تواجه الجهات الحكومية في هذا المجال. وقد تم صياغة الأسئلة بطريقة تسمح للمتلقي بالإجابة ضمن مقياس ليكرت الخماسي، حيث يمثل الرقم ١ أقصى درجة موافقة والرقم ٥ أقصى درجة رفض، بما يسهل تحويل التقييمات إلى بيانات كمية يمكن تحليلها إحصائيًا.

وقبل تطبيق الاستبيان على عينة الدراسة، تم إجراء اختبار تجريبي أولي للتأكد من وضوح الأسئلة وسهولة فهمها من قبل المستجيبين، كما تم قياس موثوقية الأداة باستخدام معامل كرونباخ ألفا لضمان اتساق الإجابات وثباتها. وبهذه الطريقة، توفر الأداة قاعدة بيانات متكاملة يمكن تحليلها باستخدام الأساليب الإحصائية الوصفية والاستدلالية، بما يعزز دقة النتائج ويسهم في اختبار الفرضيات العلمية المرتبطة بالبحث.

يمثل الاستبيان الكمي أداة محورية في هذه الدراسة، إذ لا يقتصر دوره على جمع البيانات فحسب، بل يربط بين النظرية والممارسة من خلال قياس فاعلية الاستراتيجيات المعتمدة، وتحليل أثرها على حماية المعلومات واستخدام الخدمات الرقمية في الجهات الحكومية، بما يدعم تقديم توصيات عملية قابلة للتطبيق على الواقع المحلي في المملكة العربية السعودية.

حدود البحث

• الحدود البشرية

تركز هذه الدراسة على المسؤولين التنفيذيين والإداريين والفنيين المكلفين بإدارة الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية، باعتبارهم الأطراف الأكثر معرفة باستراتيجيات إدارة المخاطر السيبرانية وفعاليتها. وتشمل هذه الفئة المديرين التنفيذيين، مدراء أقسام الأمن السيبراني، والمختصين الفنيين، حيث يمتلكون الخبرة العملية والمعرفة الكافية بتطبيق السياسات والإجراءات الأمنية الرقمية. وقد تم اختيار هذه الفئة لأنها قادرة على تقديم بيانات دقيقة وموثوقة حول الاستراتيجيات المعتمدة، مدى فاعليتها، التحديات التي تواجهها، والأثر العملي لهذه الاستراتيجيات على حماية البيانات واستمرارية الخدمات الرقمية.

• الحدود الزمانية

تقتصر الدراسة على الفترة الحالية، مع التركيز على آخر ثلاث سنوات، وذلك لمواكبة التطورات الرقمية والتكنولوجية الحديثة التي شهدتها الجهات الحكومية السعودية، خاصة في سياق برامج التحول الرقمي ورؤية المملكة ٢٠٣٠. ويأتي تحديد هذه الفترة الزمنية لضمان أن تكون البيانات حديثة وذات صلة بالواقع الرقمي الحالي، كما يعكس تقييم الفاعلية مدى جاهزية الجهات الحكومية لمواجهة التهديدات السيبرانية الحديثة، ويتيح تحليل أثر الاستراتيجيات المطبقة ضمن بيئة رقمية متطورة ومتغيرة باستمرار.

• الحدود المكانية

تتركز الدراسة على الجهات الحكومية داخل المملكة العربية السعودية التي تعتمد على أنظمة وخدمات رقمية في تقديم خدماتها للمواطنين والمستفيدين. ويشمل ذلك مجموعة من الوزارات والهيئات الحكومية والمدن الكبرى، مثل الرياض، جدة، والدمام، بهدف تمثيل التنوع في العمليات والخدمات الرقمية عبر مختلف مناطق المملكة. وقد تم تحديد هذا النطاق المكاني لضمان أن

تعكس نتائج الدراسة الواقع العملي للجهات الحكومية السعودية، مع مراعاة الخصائص التنظيمية والتقنية المحلية التي تؤثر في فاعلية تطبيق استراتيجيات إدارة المخاطر المبرانية.

الفصل الرابع

نتائج الدراسة

المقدمة

يشكل الفصل الرابع المرحلة التي تنتقل فيها الدراسة من الجانب النظري والمنهجي إلى الجانب التطبيقي، حيث يتم تحويل البيانات الميدانية إلى نتائج علمية يمكن تفسيرها والاستفادة منها في الإجابة عن أسئلة الدراسة وتحقيق أهدافها. ويهدف هذا الفصل إلى تقديم عرض علمي منظم للبيانات التي تم جمعها، ثم معالجتها باستخدام الأساليب الإحصائية المناسبة، بما يتيح استخلاص مؤشرات دقيقة تعكس واقع استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية السعودية، ومدى إسهامها في تعزيز الأمن الرقمي في ظل التحول الرقمي المتسارع.

ولا يقتصر دور هذا الفصل على عرض النتائج الرقمية، بل يمتد إلى تفسيرها وربطها بالإطار العلمي الذي استندت إليه الدراسة، مع تحليل دلالاتها العملية والإدارية، وبيان مدى توافقها مع ما توصلت إليه الأدبيات العلمية والدراسات السابقة. كما يوضح هذا الفصل الآثار المترتبة على النتائج بالنسبة للجهات الحكومية. ويرز الجوانب التي يمكن تطويرها لتعزيز فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني، بما يسهم في تحسين مستوى حماية المعلومات واستمرارية الخدمات الحكومية الرقمية، ورفع كفاءة الأداء المؤسسي في بيئة التحول الرقمي.

وتكمن أهمية هذا الفصل في كونه يمثل المحصلة النهائية لجميع مراحل البحث، فمن خلاله يتم الانتقال من البيانات الخام إلى المعرفة العلمية التي يمكن الاعتماد عليها في دعم صنع القرار ووضع السياسات. كما يسهم في تقديم استنتاجات موضوعية ومقترحات عملية قابلة للتطبيق، تساعد الجهات الحكومية على تطوير استراتيجياتها في مجال الأمن السيبراني، وتعزيز جاهزيتها لمواجهة المخاطر الرقمية الحالية والمستقبلية. وبذلك يشكل هذا الفصل قيمة علمية وتطبيقية للدراسة، إذ يربط بين النتائج الميدانية والأبعاد الاستراتيجية للتحول الرقمي، ويقدم رؤية يمكن الاستفادة منها في دعم تحقيق مستهدفات رؤية المملكة العربية السعودية ٢٠٣٠ نحو بناء حكومة رقمية آمنة ومرنة ومستدامة.

• الوصف الإحصائي للبيانات

تبين القراءات الأولية للبيانات المجمعة من مائتين وثلاثة وستين مستجيباً وجود تباين منطقي في قيم المتوسطات الحسابية والانحرافات المعيارية للمتغيرات الديموغرافية والمهنية؛ فالمتوسط الحسابي للعمر البالغ رقم مائتين وسبعة وتسعين يرافقه انحراف معياري قدره واحد فاصلة أربعة مئة وعشرة؛ وهو ما يوحي بتنوع الفئات العمرية المشاركة في الدراسة وتعدد خلقياتها العملية داخل الأجهزة الحكومية؛ كما أن اقتراب المتوسطات الحسابية لفقرات استراتيجيات الأمن السيبراني من حاجز الثلاثة فاصلة خمسة مع وجود انحرافات معيارية تتجاوز الواحد الصحيح يشير إلى حالة من عدم الاتفاق المطلق بين الموظفين حول جودة التطبيق الفعلي؛ فربما يرجع هذا التشتت في الآراء إلى اختلاف مستويات النضج الرقمي بين جهة حكومية وأخرى؛ فبينما تعيش بعض المؤسسات طفرة تقنية متقدمة قد تعاني جهات أخرى من فجوات في التنفيذ؛ وتؤكد قيمة الخطأ المعياري للمتوسط المنخفضة نسبياً دقة تقدير المجتمع الدراسي؛ فالميل العام للنتائج يسير باتجاه الموافقة على وجود استراتيجيات تقنية لكنها موافقة مشوبة بالجزر الإحصائي نظراً لقيم الالتواء السلبية التي ظهرت في معظم الفقرات؛ فالتوزيع يميل نحو القيم العليا للقياس؛ وهذا التراكم في الإجابات الإيجابية يمنع مؤشراً على وجود وعي مؤسسي عام بأهمية المخاطر السيبرانية؛ وقد تسهم هذه الحالة في تسهيل عمليات التحول الرقمي القادمة؛ فالمؤسسة التي يدرك أفرادها أهمية الأمن تكون أكثر قدرة على الصمود أمام الهجمات؛ والتباين الظاهر في فقرة البنية التقنية بمتوسط ثلاثة فاصلة واحد وخمسين وانحراف واحد فاصلة أربعة مئة يفتح الباب لتوقعات بوجود تفاوت في الإمكانيات المادية بين القطاعات المختلفة؛ فالتجهيزات التقنية لا تزال تمثل تحدياً يتطلب استثمارات مستمرة؛ والقراءة الكلية لهذا الوصف تضع حجر الأساس لفهم التداخلات المعقدة بين العنصر البشري والبنية التكنولوجية في البيئة السعودية.

جدول 1: التعليقات الإحصائية

Statistics									
Std. Error of Kurtosis	Kurtosis	Std. Error of Skewness	Skewness	Std. Deviation	Median	Std. Error of Mean	Mean	N	
								Missing	Valid
.٢٩٩	-١,٢٧٩	.١٥٠	-.٠١٣	١,٤١٠	٣,٠٠٠	.٠٨٧	٢,٩٧	٠	٢٦٣
.٢٩٩	-١,٩٣٣	.١٥٠	.٢٨٦	.٤٩٦	١,٠٠٠	.٠٣١	١,٤٣	٠	٢٦٣
.٢٩٩	-١,١٤٥	.١٥٠	-.٢٧٤	١,٣٢٢	٣,٠٠٠	.٠٨٢	٣,٤٠	٠	٢٦٣

٢٦٣	٠	٣,٥٤	٠,٨٣	٤,٠٠	١,٣٤٤	-٦٠٧	١٥٠	-٩١٩	٢٩٩	تطبيق الجهة الحكومية استراتيجيات وأمن إدارة مخاطر الأمن الميزاني
٢٦٣	٠	٣,١٣	٠,٨٦	٤,٠٠	١,٣٩٩	-٥٣٧	١٥٠	-١,٠٦٢	٢٩٩	يتم تحديث استراتيجيات الأمن الميزاني بشكل توري أمثلة التحديات الحديثة
٢٦٣	٠	٣,٥٤	٠,٨٧	٤,٠٠	١,٤٠٥	-٦١٤	١٥٠	-٩٧٣	٢٩٩	تتمتع الجهة على معلومات علمية الجهة وتقيم المخاطر السيبرانية
٢٦٣	٠	٣,٤١	٠,٩٣	٤,٠٠	١,٥١٥	-٤١٤	١٥٠	-١,٣١٧	٢٩٩	تسهم استراتيجيات إدارة المخاطر في تقليل الحوادث وقوع الهجمات السيبرانية
٢٦٣	٠	٣,٥٤	٠,٧٩	٤,٠٠	١,٢٨٣	-٦٠٠	١٥٠	-٨٠٠	٢٩٩	تساعد استراتيجيات الأمن السيبراني في ضمان استمرارية الأصول والخدمات المعتمدة
٢٦٣	٠	٣,٥٢	٠,٨٦	٤,٠٠	١,٤٠٠	-٥٩٩	١٥٠	-٩٩٨	٢٩٩	يتم تطبيق استراتيجيات إدارة المخاطر في تعزيز أمن البيئة الرقمية للجهة
٢٦٣	٠	٣,٥١	٠,٨٦	٤,٠٠	١,٤٠٠	-٥٨٢	١٥٠	-١,٠٢٩	٢٩٩	تمتلك الجهة خطة مخطوطة لأمن الأمن الميزاني
٢٦٣	٠	٣,٢٤	٠,٩٢	٤,٠٠	١,٤٩٥	-٣٦٦	١٥٠	-١,٣٣٥	٢٩٩	للتحكم الجهة تقنيات حديثة لرصد والكشف التهديدات الميزانية
٢٦٣	٠	٣,٤٩	٠,٨٣	٤,٠٠	١,٣٥٣	-٥٣٣	١٥٠	-١,٠٠٩	٢٩٩	يتم تحديث الأنظمة الأمنية بصورة مستمرة لمواجهة المخاطر الحديثة

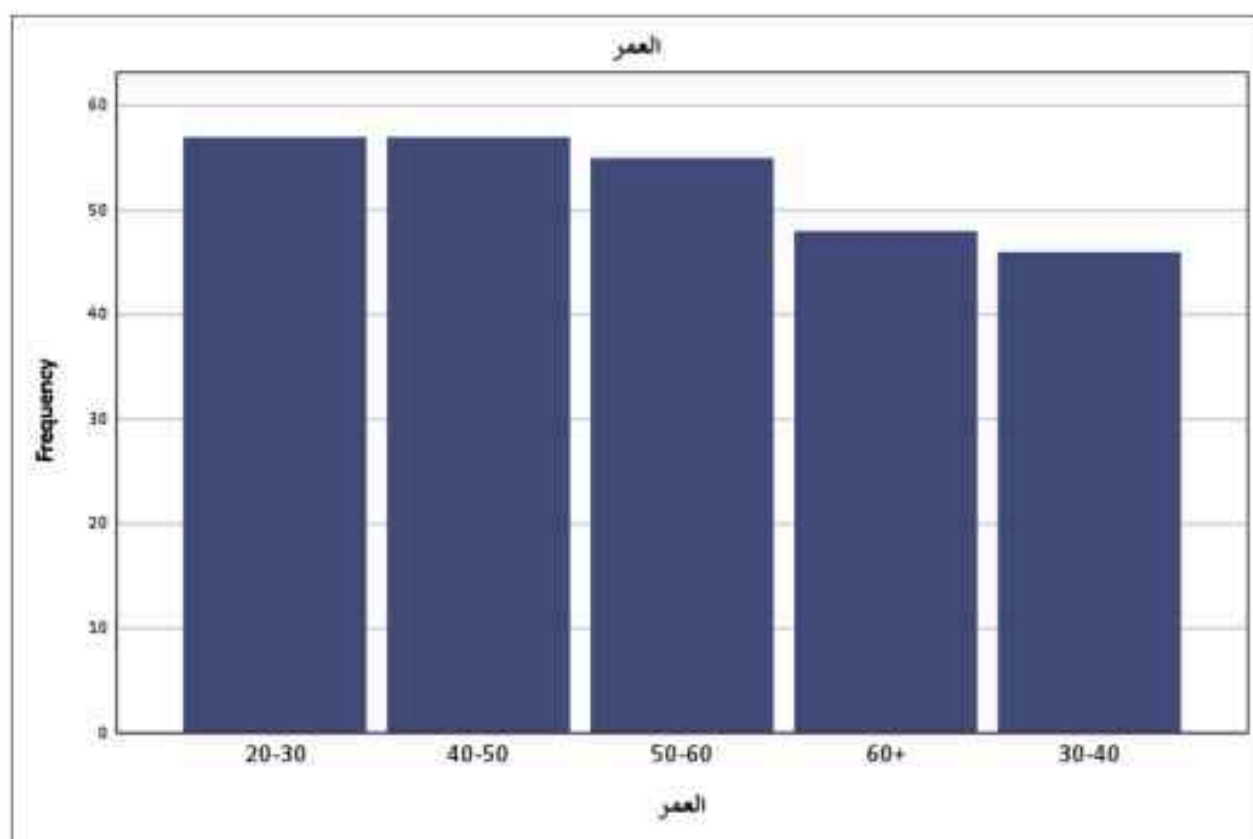
٢٦٣	٠	٣,٤٨	٠,٨٤	٤,١٠٠	١,٣٥٩	٠,٥٤١	١٥٠	٠,٩٨٠	٢٩٩	تسليم البنية التحتية في رفع كفاءة الإستجابة للتحديات السيبرانية
٢٦٣	٠	٣,٤٩	٠,٨٩	٤,١٠٠	١,٤٣٥	٠,٥١٥	١٥٠	٠,١٦٥	٢٩٩	تسليم البنية التحتية المتقدمة في حماية البيانات والأصول الرقمية
٢٦٣	٠	٣,٣٧	٠,٩٥	٤,١٠٠	١,٥٤٧	٠,٣٩٧	١٥٠	٠,١٠٦	٢٩٩	تسليم التحضيرية التقنية في تعزيز فعالية إدارة مخاطر الأمن السيبراني
٢٦٣	٠	٣,٥٠	٠,٨٣	٤,١٠٠	١,٣٤٨	٠,٥١٠	١٥٠	٠,١٠٨	٢٩٩	توفر الجهة برامج التدريب منتظمة في مجال الأمن السيبراني للعاملين
٢٦٣	٠	٣,٥٥	٠,٨٦	٤,١٠٠	١,٣٨٩	٠,٥٧٣	١٥٠	٠,١٣٣	٢٩٩	توفر كورس بالمختبر السيبرانية عن جميع الموظفين
٢٦٣	٠	٣,٣٥	٠,٩١	٤,١٠٠	١,٤٧٣	٠,٣٥٣	١٥٠	٠,١٥٢	٢٩٩	تتقدم المجلس بمخطط سياسات وأجراءات الأمن السيبراني
٢٦٣	٠	٣,٥٤	٠,٨٤	٤,١٠٠	١,٣٦٤	٠,٦٤٤	١٥٠	٠,٨٦٠	٢٩٩	تسليم التدريب والتوعية في الحد من الأخطاء البشرية المرتبطة بالأمن السيبراني
٢٦٣	٠	٣,٥٩	٠,٨٠	٤,١٠٠	١,٣٠١	٠,٦٤٦	١٥٠	٠,٧١٠	٢٩٩	تسليم استراتيجيات إدارة مخاطر الأمن السيبراني في تعزيز فعالية إدارة المخاطر في الجهات الحكومية بالمملكة العربية السعودية في ضوء التحول الرقمي

• العمر

تكشف التكرارات المرصودة للفئات العمرية عن توزيع متوازن بشكل مثير للاهتمام داخل عينة الدراسة: فالفئة العمرية من عشرين إلى ثلاثين عاماً والمنتمية للجيل الرقمي الحديث حصدت سبعة وخمسين تكراراً بنسبة واحد وعشرين فاصلة سبعة بالمئة؛ وهي ذات النسبة والتكرار التي حققها الفئة من أربعين إلى خمسين عاماً؛ فالمؤسسات الحكومية تبدو مزيجاً متناغماً بين طاقة الشباب وخبرة الكوادر القيادية المتوسطة؛ وقد يمنح هذا التوازن بيئة العمل قدرة فريدة على دمج الأفكار الابتكارية مع ضوابط الحوكمة الرصينة؛ وتأتي الفئة من خمسين إلى ستين عاماً بنسبة عشرين فاصلة تسعة بالمئة لتؤكد حضور الخبرة الطويلة في مراكز اتخاذ القرار؛ فربما تلعب هذه الفئة دوراً جوهرياً في ضبط إيقاع إدارة المخاطر من منظور استراتيجي تاريخي؛ بينما تسهم الفئة الشابّة في تطبيق الحلول التقنية المعاصرة؛ فالتوزيع التكراري الذي يشمل ثمانية عشر فاصلة ثلاثة بالمئة لمن هم فوق الستين وسبعة عشر فاصلة خمسة بالمئة للفئة من ثلاثين إلى أربعين يكمل الصورة الشمولية للقوى العاملة؛ فوجود كافة الأجيال في منظومة الأمن السيبراني يقلل من احتمالات الفجوات المعرفية؛ فالخبرة الإدارية تحمي من التهور التقني والشباب يحمون من الجمود الإجرائي؛ وهذه التوليفة البشرية تحتل مستقبلاً واعداً لاستقرار السياسات الأمنية؛ فالتواصل بين هذه الأجيال قد يولد ثقافة مؤسسية متينة لمواجهة التحديات؛ والبيانات بهذا التوزيع تدعم فرضية شمولية الدراسة وقدرتها على تمثيل وجهات نظر متباينة تعبر عن واقع الهيكل الوظيفي في المملكة؛ فالتنوع العمري يعد صمام أمان لضمان استدامة المعرفة ونقلها بين الأجيال المختلفة في تخصصات حساسة كالأمن السيبراني.

جدول 2: التحليل الإحصائي للعمر

العمر					
	Cumulative Percent	Valid Percent	Percent	Frequency	
Valid	٢١,٧	٢١,٧	٢١,٧	٥٧	٢٠- ٣٠
	٤٣,٣	٢١,٧	٢١,٧	٥٧	٤٠- ٥٠
	٦٤,٣	٢٠,٩	٢٠,٩	٥٥	٥٠- ٦٠
	٨٢,٥	١٨,٣	١٨,٣	٤٨	٦٠+
	١٠٠,٠	١٧,٥	١٧,٥	٤٦	٣٠- ٤٠
		١٠٠,٠	١٠٠,٠	٢٦٣	Total



شكل توضيحي 1: التمثيل البياني للعمر

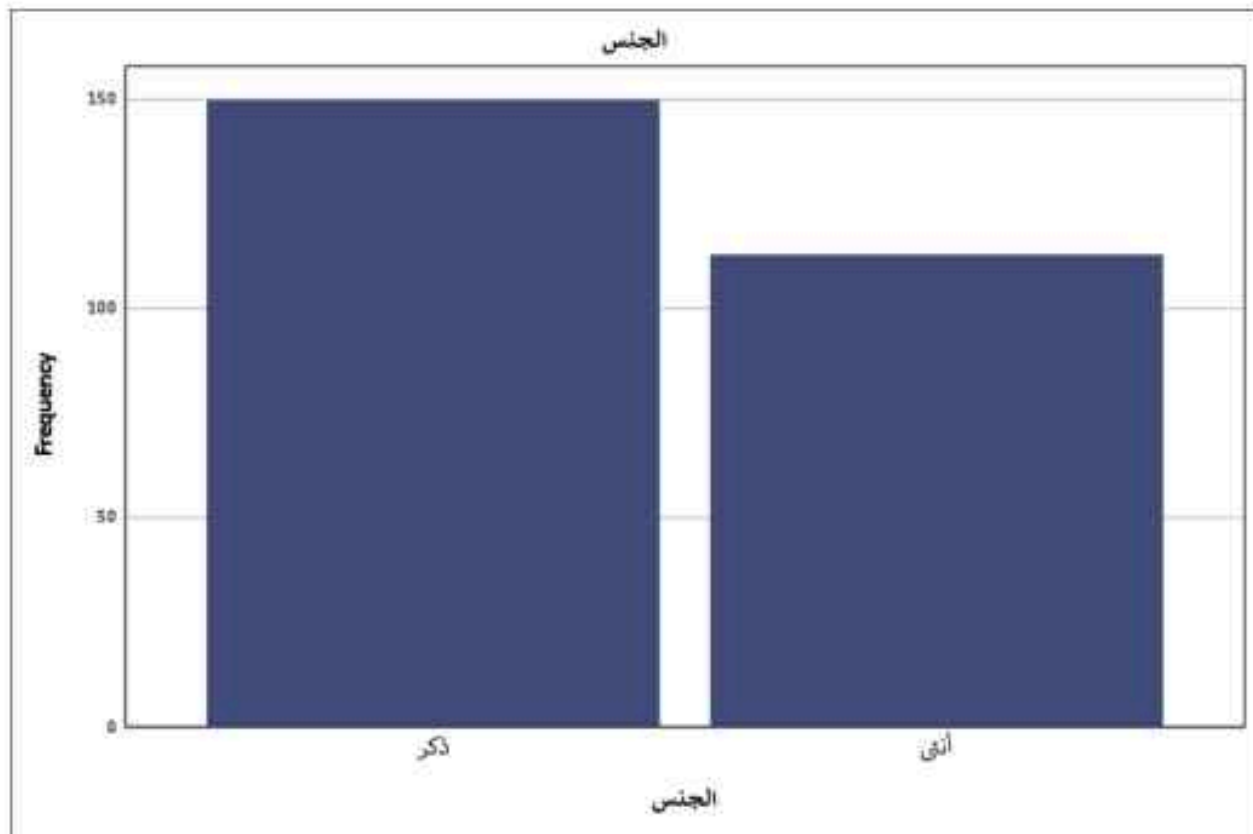
• الجنس

يبرز التوزيع النوعي للمشاركين غلبة العنصر الرجالي في قطاع الأمن السيبراني وإدارة المخاطر بالجهات الحكومية؛ فعدد الذكور بلغ مئة وخمسين مشاركاً بنسبة سبعة وخمسين بالمئة؛ مقابل مئة وثلاثة عشر من الإناث بنسبة ثلاثة وأربعين بالمئة؛ وتلك الأرقام تعطي انطباعاً عن زيادة مطردة في مشاركة المرأة في المجالات التقنية المعقدة داخل المملكة؛ فالفجوة بين الجنسين تبدو ضيقة جداً في ظل التوجهات الوطنية لتمكين الكفاءات النسائية؛ وقد يسهم هذا التقارب في خلق بيئة عمل متنوعة الرؤى؛ فالدراسات السلوكية غالباً ما تلمح إلى أن التنوع في فرق إدارة الأزمات يؤدي إلى تحليل أكثر دقة للمخاطر؛ فربما تمتلك الموظفات زوايا تقييم تختلف عن زملائهم الرجال في الجوانب المتعلقة بالامتثال والدقة الإجرائية؛ بينما قد يميل الرجال نحو الحلول التقنية المباشرة؛ فالتكامل بين التوجهين يدعم فعالية إدارة المخاطر السيبرانية بشكل شمولي؛ والبيانات تؤكد أن المرأة لم تعد بعيدة عن مراكز العمل التقني الحساس؛ فالثلاثة والأربعون بالمئة يمثلون كتلة حرجة قادرة على التأثير في صياغة السياسات الأمنية؛ ولعل هذا الوجود القوي يعكس نجاح البرامج التدريبية الموجهة للجنسين؛ فالمساواة في العينة تعزز من مصداقية

النتائج وتعميمها على مجتمع الدراسة: فمن المحتمل أن يكون الوعي بالمخاطر السيبرانية عابراً للجنس داخل المؤسسات الحكومية المتطورة؛ والتوازن النسبي الحاصل يساعد في استقرار المنظومة الإدارية وتوزيع المسؤوليات؛ فالتحديات الأمنية تتطلب تكاتف كافة القوى البشرية المتاحة دون استثناء؛ وهذا الرقم يقدم دليلاً واقعياً على تحول الثقافة المهنية في القطاع العام نحو الشمولية والاحترافية التقنية للجنسين على حد سواء.

جدول 3: التحليل الإحصائي للجنس

الجنس					
Cumulative Percent	Valid Percent	Percent	Frequency		
٥٧,٠	٥٧,٠	٥٧,٠	١٥٠	ذكر	Valid
١٠٠,٠	٤٣,٠	٤٣,٠	١١٣	أنثى	
	١٠٠,٠	١٠٠,٠	٢٦٣	Total	



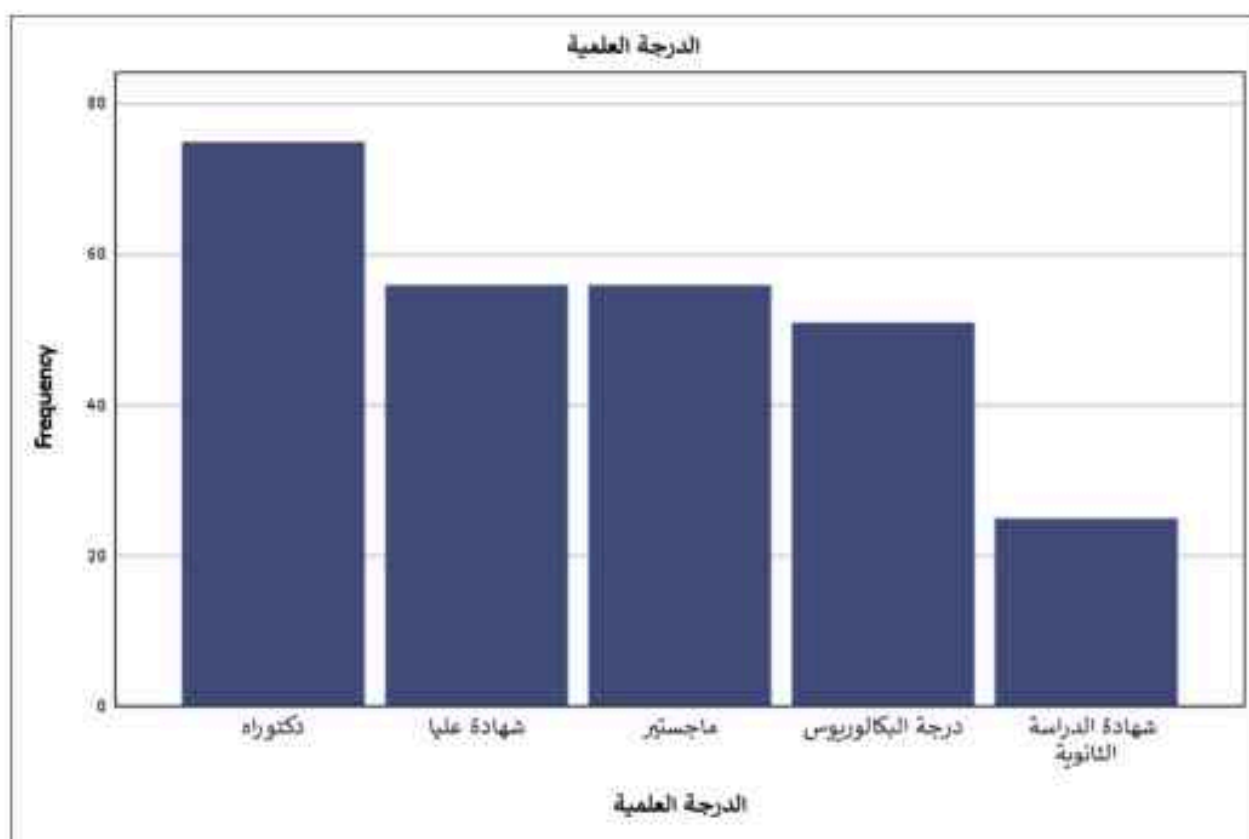
شكل توضيحي 2: التمثيل البياني للجنس

• الدرجة العلمية

تظهر المستويات التعليمية للمستجيبين ارتفاعاً ملحوظاً في التحصيل الأكاديمي؛ فنسبة الحاصلين على درجة الدكتوراه وصلت إلى ثمانية وعشرين فاصلة خمسة بالمئة بواقع خمسة وسبعين مشاركاً؛ وتبعها الحاصلون على الشهادات العليا والمجستير بنسبة واحد وعشرين فاصلة ثلاثة بالمئة لكل منهما؛ فالعينة تنسم بصيغة أكاديمية تخصصية عالية جداً؛ ووجود أكثر من سبعين بالمئة من المشاركين يحملون درجات علمية فوق الجامعية يمنح نتائج الدراسة وزناً معرفياً كبيراً؛ فربما تعتمد الجهات الحكومية في وظائف الأمن السيبراني على معايير استقطاب صارمة تفضل المؤهلات العليا؛ وهذا الارتفاع في المستوى التعليمي قد يفسر الميل نحو الموافقة على المنهجيات العلمية في إدارة المخاطر؛ فالباحث الأكاديمي يكون أكثر تقدراً للإجراءات المنهجية المتبعة؛ بينما نجد أن نسبة حملة البكالوريوس بلغت تسعة عشر فاصلة أربعة بالمئة؛ وتقل النسبة كثيراً لحملة الثانوية لتصل إلى تسعة فاصلة خمسة بالمئة؛ فالتخصص والتعمق العلمي هما السمتان الغاليتان على القوى البشرية المعنية بحماية البيئة الرقمية؛ وقد ينعكس هذا المستوى التعليمي المرموق على جودة التقارير الأمنية ودقة رصد التهديدات؛ فالعقلية المدربة على البحث العلمي هي الأقدر على فهم تعقيدات الفضاء السيبراني؛ ولربما يشير ذلك أيضاً إلى استثمار الدولة الواسع في تعليم الكوادر الوطنية بمجالات التقنية؛ فالمعرفة العلمية هي الدرع الأول في مواجهة الهجمات المبتكرة؛ والبيانات هنا توفر طمأنينة إحصائية بأن الآراء المستفادّة صادرة عن خبرات متعلمة ومدركة لأبعاد التحديات التقنية؛ فالمستوى التعليمي العالي يقلل من احتمالات الفهم الخاطئ لسياسات الأمن المعقدة ويحفز على الالتزام بها.

جدول 4: التوزيع الإحصائي للدرجة العلمية

الدرجة العلمية					
Cumulative Percent	Valid Percent	Percent	Frequency		
٢٨,٥	٢٨,٥	٢٨,٥	٧٥	دكتوراه	Valid
٤٩,٨	٢١,٣	٢١,٣	٥٦	شهادة عليا	
٧١,١	٢١,٣	٢١,٣	٥٦	ماجستير	
٩٠,٥	١٩,٤	١٩,٤	٥١	درجة البكالوريوس	
١٠٠,٠	٩,٥	٩,٥	٢٥	شهادة الدراسة الثانوية	
	١٠٠,٠	١٠٠,٠	٢٦٣	Total	



شكل توضيحي 3: التمثيل البياني للدرجة العلمية

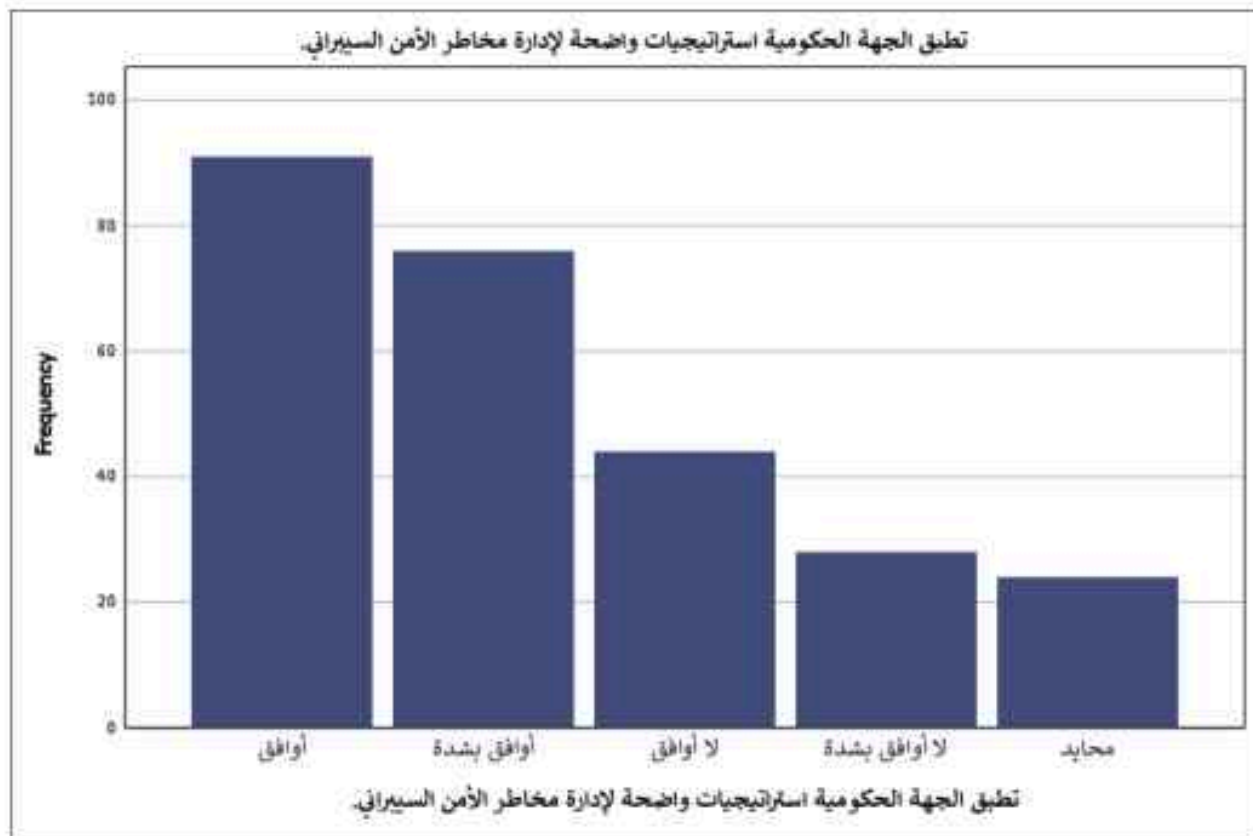
• **تطبيق الجهة الحكومية استراتيجيات واضحة لإدارة مخاطر الأمن السبيري.**

تحصلت هذه الفقرة على متوسط حسابي قدره ثلاثة فاصلة أربعة وخمسين؛ وهو ما يضعها في خانة الموافقة العامة لدى غالبية المستجيبين؛ فالتكرارات توضح أن أربعة وثلاثين فاصلة ستة بالمتن وافقوا؛ وثمانية وعشرين فاصلة تسعة بالمتن وافقوا بشدة؛ فالكثلة الإيجابية تتجاوز الثلاثة والستين بالمتن من إجمالي العينة؛ وهذا التوجه يبعث برسالة مفادها أن الاستراتيجيات لم تعد حبراً على ورق في الأروقة الحكومية؛ فالتخطيط الواضح يبدو ملموساً للموظفين في واقعهم اليومي؛ غير أن وجود ستة عشر فاصلة سبعة بالمتن من غير الموافقين وعشرة فاصلة ستة بالمتن من غير الموافقين بشدة يستدعي وقفة تحليلية؛ فربما تعاني بعض الأقسام داخل الجهة من عدم وصول الرؤية الاستراتيجية إليها؛ أو قد يكون هناك تفاوت في فهم ماهية "الاستراتيجية الواضحة" بين المستويات الوظيفية؛ فالانحراف المعياري البالغ واحد فاصلة ثلاثمئة وأربعة وأربعين يؤكد هذا التباين في الإدراك؛ فالتشقت في الإجابات يشير إلى وجود فجوات تواصلية محتملة داخل المنظمة؛ فبينما يرى البعض وضوحاً كاملاً؛ يشعر آخرون بضبابية الإجراءات؛ ولعل غياب التوافق التام يعود إلى حداثة تطبيق بعض المعايير الدولية في بعض القطاعات؛ فالتحول

الرقعي المتسارع قد يسبق أحياناً قدرة الأفراد على استيعاب الاستراتيجيات الجديدة: والقيمة المتوسطة تشير إلى وضع جيد لكنه يحتاج إلى تعزيز لتقليل الفئة الراضية أو المحايدة البالغة تسعة فاصلة واحد بالمئة: فالوضوح الاستراتيجي هو الركيزة التي تنبثق منها كافة الجهود الأمنية الناجحة: وتكرار "أوافق بشدة" كخيار ثانٍ يعزز الثقة في وجود توجه قيادي قوي نحو مؤسسة إدارة المخاطر: فالارتقاء بهذا المتوسط مستقبلاً يتطلب جهوداً تواصلية لتعميم الاستراتيجيات على كافة المستويات الوظيفية لضمان شمولية التطبيق.

جدول 5 : التحليل الإحصائي للتطبيق للجهة الحكومية استراتيجيات واضحة لإدارة مخاطر الأمن السيبراني.

تطبيق الجهة الحكومية استراتيجيات واضحة لإدارة مخاطر الأمن السيبراني.					
	Frequency	Percent	Valid Percent	Cumulative Percent	
أوافق	٩١	٣٤,٦	٣٤,٦	٣٤,٦	Valid
أوافق بشدة	٧٦	٢٨,٩	٢٨,٩	٦٣,٥	
لا أوافق	٤٤	١٦,٧	١٦,٧	٨٠,٢	
لا أوافق بشدة	٢٨	١٠,٦	١٠,٦	٩٠,٩	
محايد	٢٤	٩,١	٩,١	١٠٠,٠	
Total	٢٦٣	١٠٠,٠	١٠٠,٠		



شكل توضيحي 4: التعليل البياني لتطبيق الجهة الحكومية استراتيجيات واضحة لإدارة مخاطر الأمن السيبراني.

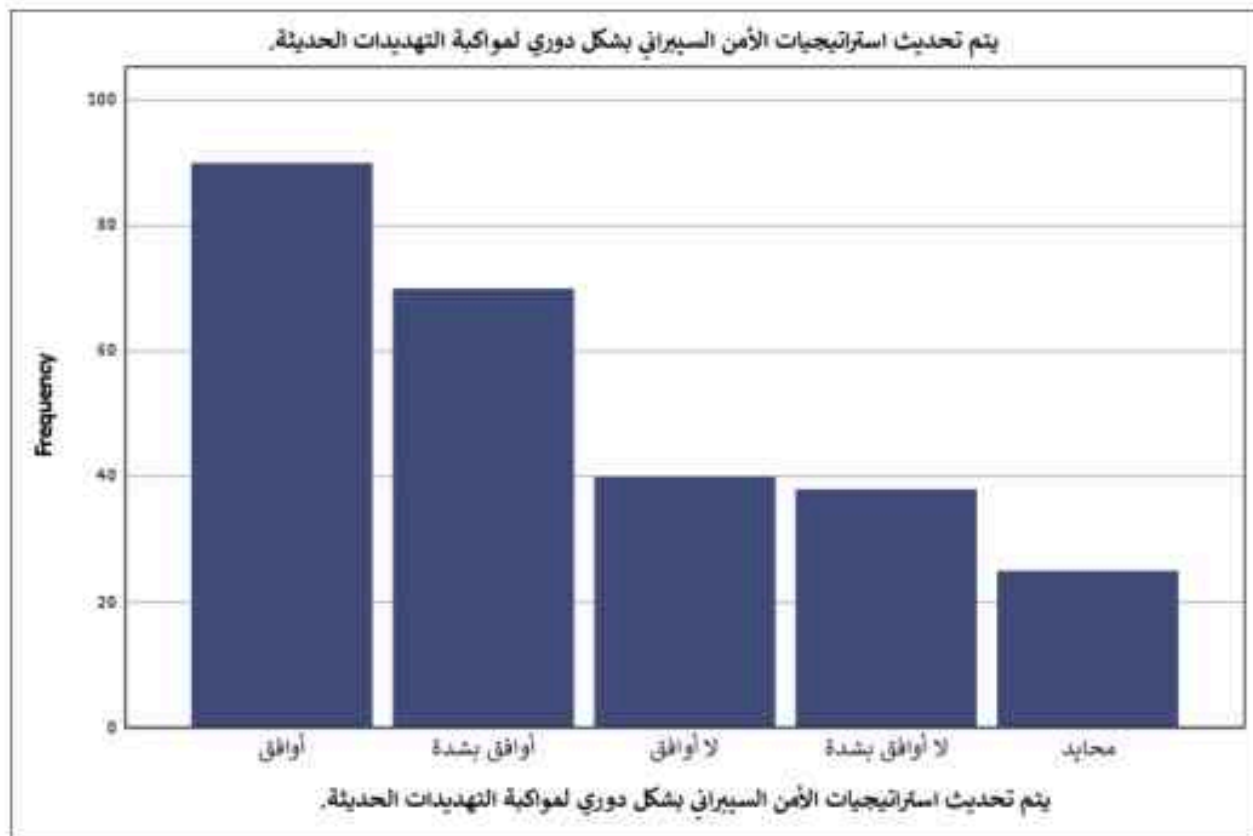
- يتم تحديث استراتيجيات الأمن السيبراني بشكل دوري لمواكبة التهديدات الحديثة.

تعكس النتائج الحاصلة على متوسط ثلاثة فاصلة ثلاثة وأربعين وانحراف واحد فاصلة ثلاثمئة وتسعة وتسعين وعياً مؤسسياً بضرورة التحديث المستمر؛ فالموافقون والموافقون بشدة يشكلون ستين فاصلة ثمانية بالمئة من العينة؛ وهذه النسبة تبرهن على أن الجهات الحكومية لا تكتفي بوضع الخطط الساكنة بل تسعى للملاحقة التطورات المتسارعة في عالم التهديدات؛ فالمرونة في تحديث الاستراتيجيات هي ما يمنح المنظومة قدرة على الصمود؛ وربما يفسر حصول خيار "لا أوافق" و"لا أوافق بشدة" على ما يقارب الثلاثين بالمئة مجتمعين وجود تحديثات بيروقراطية قد تعيق سرعة التحديث في بعض الأحيان؛ فالإجراءات الحكومية الطويلة قد لا تتناسب مع سرعة تولد الفيروسات والبرمجيات الخبيثة؛ فالتشتت الظاهر في الإجابات يلمح إلى أن عملية التحديث ليست منتظمة بنفس الوتيرة في جميع القطاعات التابعة للجهة؛ فربما تركز التحديثات على الأنظمة الجرجة فقط وتهمل الأنظمة الفرعية؛ والبيانات تظهر أن تسعة فاصلة خمسة بالمئة اختلفوا الجواب؛ ولعل ذلك ناتج عن عدم اطلاع هؤلاء الموظفين على كواليس الإدارة العليا للأمن؛ فالتحديث الدوري يتطلب ميزانيات وكوادر بشرية مؤهلة؛ وهذا الرقم المتوسط يضع الإدارة أمام تحدي تقليص الفجوة الزمنية بين ظهور التهديد وتحديث الاستراتيجية المقابلة له؛ فالاستراتيجية القديمة قد تصبح

عبئاً أمنياً إذا لم تواكب الواقع؛ والميل العام نحو الموافقة يعطي شرعية للجهود المبذولة حالياً؛ فالمستجيبون يشعرون بوجود حركة تحديثية وإن كانت غير مكتملة في نظر البعض؛ وهذه القراءة تستوجب مراجعة آليات نشر التحديثات وإشراك الموظفين في معرفة التطورات الجديدة؛ فالتوعية بالتحديث لا تقل أهمية عن التحديث ذاته لضمان تجاوب العنصر البشري مع التغييرات التقنية الطارئة.

جدول 6 : التحليل الإحصائي لتحديث استراتيجيات الأمن السيبراني بشكل دوري لمراقبة التهديدات الحديثة.

يتم تحديث استراتيجيات الأمن السيبراني بشكل دوري لمواكبة التهديدات الحديثة.					
	Frequency	Percent	Valid Percent	Cumulative Percent	
أوافق	٩٠	٣٤,٢	٣٤,٢	٣٤,٢	Valid
أوافق بشدة	٧٠	٢٦,٦	٢٦,٦	٦٠,٨	
لا أوافق	٤٠	١٥,٢	١٥,٢	٧٦,٠	
لا أوافق بشدة	٣٨	١٤,٤	١٤,٤	٩٠,٥	
محايد	٢٥	٩,٥	٩,٥	١٠٠,٠	
Total	٢٦٣	١٠٠,٠	١٠٠,٠		



شكل 5: التمثيل البياني لـ تحديث استراتيجيات الأمن السيبراني بشكل دوري لمواجهة التهديدات الحديثة.

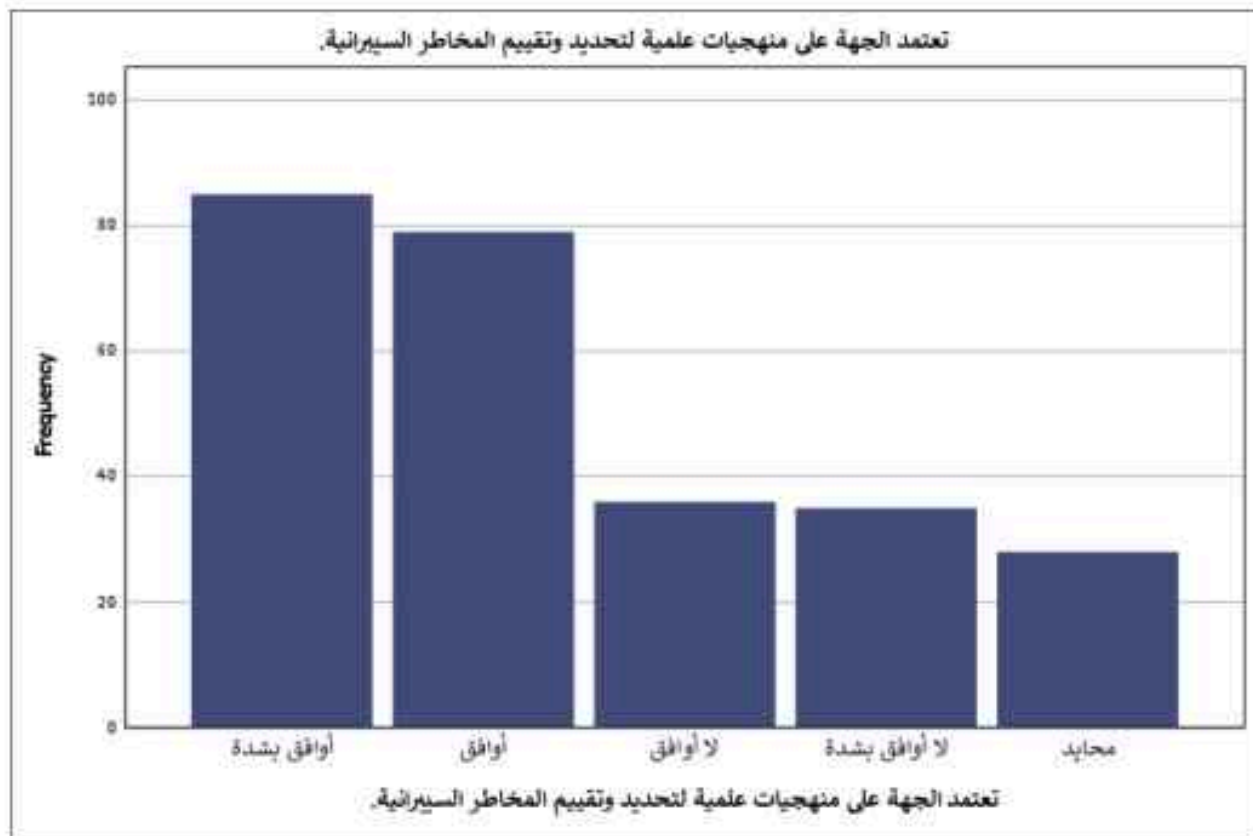
• تعتمد الجهة على منهجيات علمية لتحديد وتقييم المخاطر السيبرانية.

يشير المتوسط الحسابي البالغ ثلاثة فاصلة أربعة وخمسين إلى قناعة عامة لدى المبحوثين بجدية المعايير المتبعة؛ فخيار "أوافق بشدة" تصدر المشهد باثنين وثلاثين فاصلة ثلاثة بالمنة؛ متبوعاً بخيار "أوافق" بنسبة ثلاثين بالمنة؛ فالمجموع الذي يتخطى اثنين وستين بالمنة يعزز فرضية التحول نحو الإدارة العلمية للمخاطر بدلاً من الاجتهادات الشخصية؛ فاستخدام أطر العمل العالمية مثل (NIST) أو (ISO) قد يكون هو المقصود بهذه المنهجيات في الواقع العملي؛ وربما يرجع الانحراف المعياري المقدر بواحد فاصلة أربعة منة وخمسة إلى تباين عمق الفهم لهذه المنهجيات بين الموظفين التقنيين والإداريين؛ فالإداري قد يرى المنهجية كإجراء روتيني بينما يراها التقني كضرورة فنية؛ والبيانات تكشف أن سبعة وعشرين بالمنة تقريباً يتوزعون بين الرفض المطلق أو الجزئي؛ ولعل ذلك يشير إلى وجود أنظمة قديمة في بعض القطاعات لا تزال تعمل بآليات تقييم بدائية؛ فالفجوة بين النظرية العلمية والتطبيق الفعلي قد تظهر في البيانات ذات الإرث التقني القديم؛ وتظهر فئة المجاهدين بنسبة عشرة فاصلة ستة بالمنة ككتلة تحتاج إلى برامج توعوية لتعريفها بالأسس العلمية التي تقوم عليها حماية البيانات؛ فالمعرفة بالمنهجية تزيد من ثقة الموظف في أمان بيئته الرقمية؛ والارتباط بين الدرجة العلمية العالية للعينة وهذه النتائج يبدو منطقياً؛ فحملة الدكتوراه والمجستير هم

الأكثر قدرة على تمييز المنهج العلمي وتثمينه: فالنتائج في مجملها إيجابية وتدفع باتجاه مأسسة التقييم الدوري للمخاطر: فالاستناد إلى العلم يقلل من هامش الخطأ البشري في تقدير جسامة التهديدات: وهذا الرقم يعطي ضوءاً أخضر لصناع القرار للاستمرار في تطوير الأدوات المنهجية: فالمجتمع الدراسي يشعر بقيمة هذا التوجه ويؤيد استمراره لضمان حماية وطنية شاملة.

جدول 7: التحليل الإحصائي لاعتماد الجهة على منهجيات علمية لتحديد وتقييم المخاطر السيبرانية.

تعتمد الجهة على منهجيات علمية لتحديد وتقييم المخاطر السيبرانية.					
	Frequency	Percent	Valid Percent	Cumulative Percent	
أوافق بشدة	٨٥	٣٢,٣	٣٢,٣	٣٢,٣	Valid
أوافق	٧٩	٣٠,٠	٣٠,٠	٦٢,٤	
لا أوافق	٣٦	١٣,٧	١٣,٧	٧٦,٠	
لا أوافق بشدة	٣٥	١٣,٣	١٣,٣	٨٩,٤	
محايد	٢٨	١٠,٦	١٠,٦	١٠٠,٠	
Total	٢٦٣	١٠٠,٠	١٠٠,٠		



شكل توضيحي 6: التمثيل البياني لاعتماد الجهة على منهجيات علمية لتحديد وتقييم المخاطر السيبرانية.

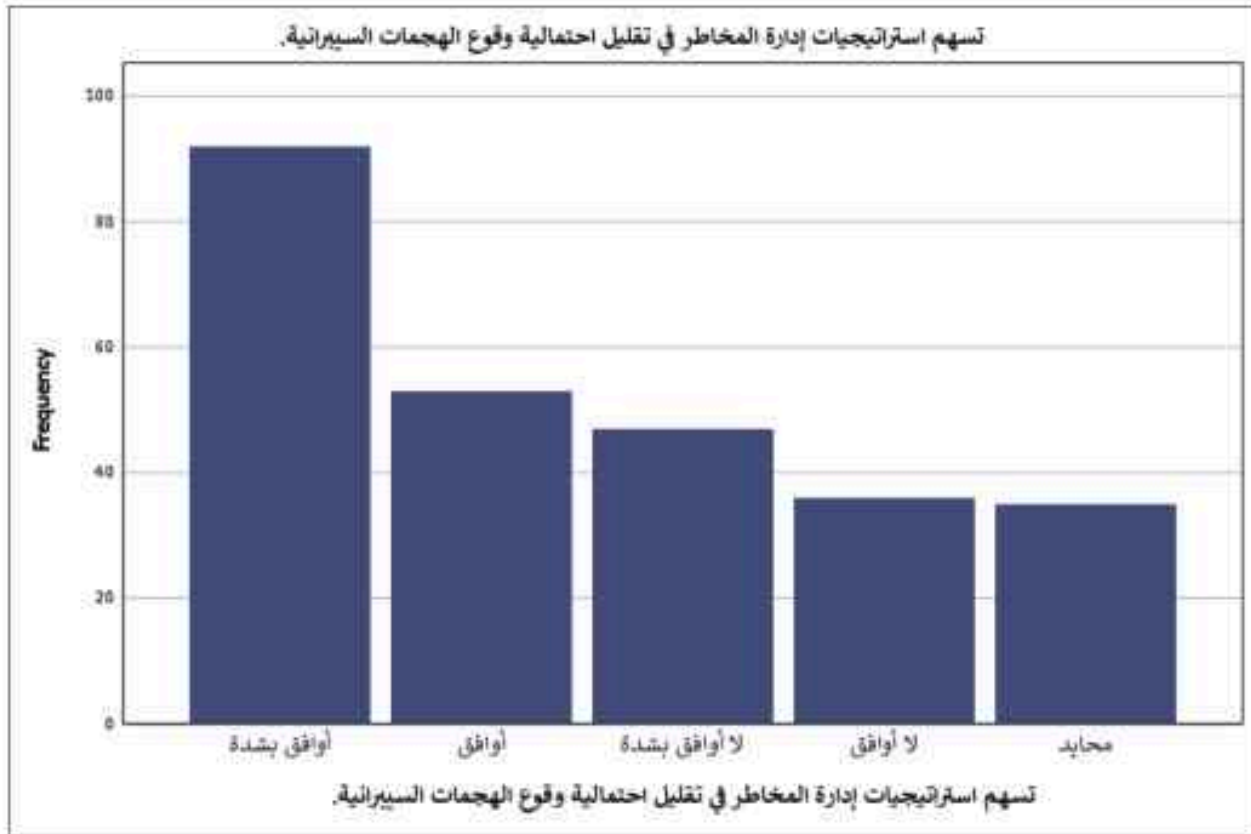
• تسهم استراتيجيات إدارة المخاطر في تقليل احتمالية وقوع الهجمات السيبرانية.

تتجلى أهمية التخطيط الوقائي في هذه الفقرة التي سجلت متوسطاً قدره ثلاثة فاصلة واحد وأربعين؛ ورغم أن خيار "أوافق بشدة" نال النسبة الأعلى بخمسة وثلاثين بالمئة؛ إلا أن هناك تشتتاً ملحوظاً يعكسه الانحراف المعياري المرتفع والبالغ واحد فاصلة خمسمئة وخمسة عشر؛ وهو أعلى انحراف مسجل في هذه الجزئية؛ وهذا التباين الكبير يوحي بوجود انقسام في الرؤى حول الجدوى الفعلية للاستراتيجيات في منع الهجمات؛ فربما يرى فريق أن الهجمات قدر محتوم لا تمنعه الخطط بل تخفف من أثاره فقط؛ بينما يرى فريق آخر أن الاستراتيجية هي الحصن الأول والمانع الحقيقي؛ فالبيانات تظهر أن سبعة عشر فاصلة تسعة بالمئة لا يوافقون بشدة؛ وثلاثة عشر فاصلة سبعة بالمئة لا يوافقون؛ فالمقاومة الفكرية لفعالية الاستراتيجيات تصل إلى الثلث تقريباً؛ ولعل هذا الإحباط الإحصائي ناتج عن تجارب سابقة لخرق أمني حدث رغم وجود خطط قائمة؛ فالميدان العملي قد يواجه تحديات تفوق ما هو مرسوم على الورق؛ وتبرز نسبة الحياد البالغة ثلاثة عشر فاصلة ثلاثة بالمئة لتعكس حالة من عدم اليقين؛ فالأمن السيبراني بطبعه احتمالي ولا توجد فيه ضمانات مطلقة؛ فالموظف الذي يرى الهجمات تتطور يومياً قد يشكك في قدرة أي استراتيجية ثابتة على صدده؛ ومع ذلك فالموافقون يشكلون الأغلبية البسيطة بخمسة وخمسين بالمئة؛ فالثقة

لا تزال موجودة في جدوى العمل الاستراتيجي كأداة لتقليل الاحتمالات: والنتائج تدعو لإعادة النظر في كيفية عرض قصص النجاح الأمنية على الموظفين لتعزيز ثقتهم في الاستراتيجيات المتبعة؛ فالافتناع بجدوى الدفاع هو أول خطوات النجاح؛ وهذه القراءات تحتمل ضرورة دمج الاستراتيجيات بأدوات تقنية تنفيذية تجعل أثرها ملموساً وليس مجرد تنظير إداري بعيد عن الواقع النقفي.

جدول 8: التحليل الإحصائي لمساهمة استراتيجيات إدارة المخاطر في تقليل احتمالية وقوع الهجمات السيبرانية.

تسهم استراتيجيات إدارة المخاطر في تقليل احتمالية وقوع الهجمات السيبرانية.					
	Frequency	Percent	Valid Percent	Cumulative Percent	
أوافق بشدة	٩٢	٣٥,٠	٣٥,٠	٣٥,٠	Valid
أوافق	٥٣	٢٠,٢	٢٠,٢	٥٥,١	
لا أوافق بشدة	٤٧	١٧,٩	١٧,٩	٧٣,٠	
لا أوافق	٣٦	١٣,٧	١٣,٧	٨٦,٧	
محايد	٣٥	١٣,٣	١٣,٣	١٠٠,٠	
Total	٢٦٣	١٠٠,٠	١٠٠,٠		



شكل توضيحي 7: التمثيل البياني للمساهمة استراتيجيات إدارة المخاطر في تقليل احتمالية وقوع الهجمات السيبرانية.

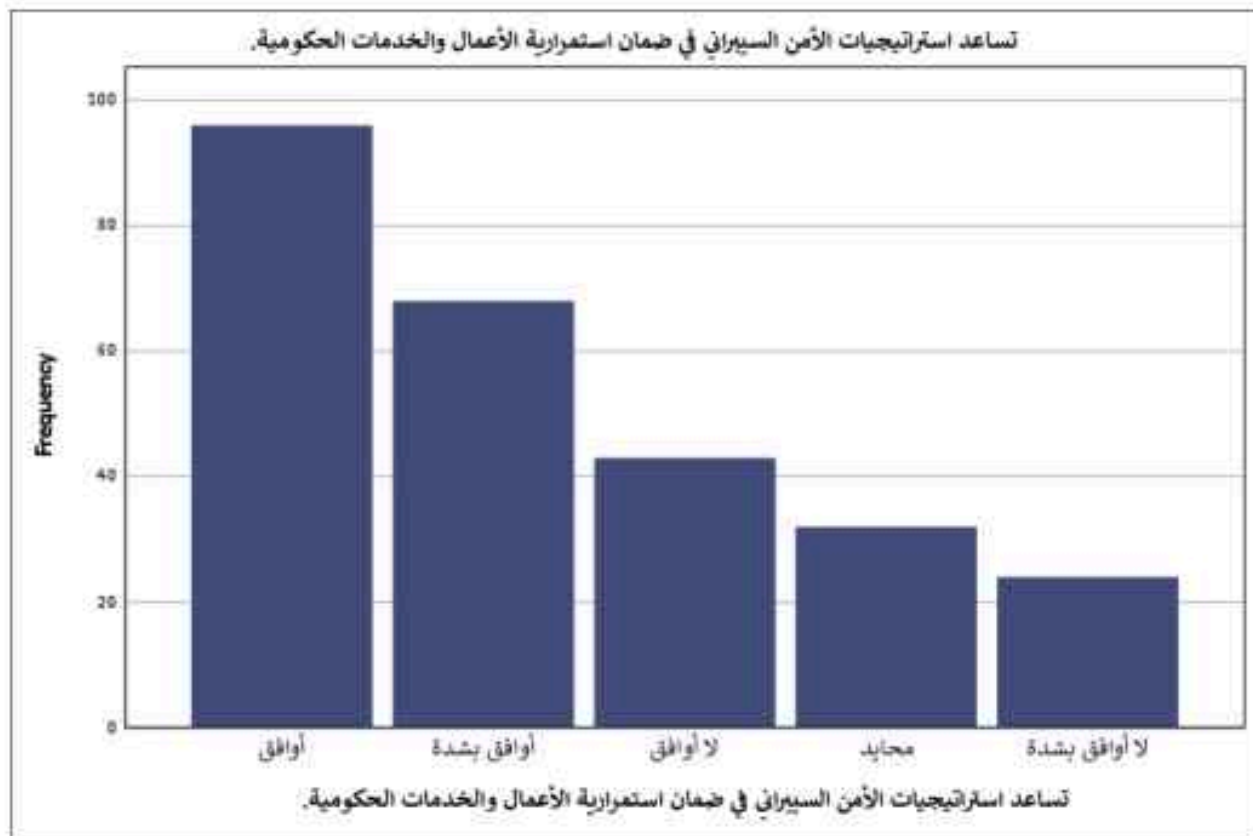
• تساعد استراتيجيات الأمن السيبراني في ضمان استمرارية الأعمال والخدمات الحكومية.

تحقق هذه الفقرة متوسطاً حسابياً قوياً يصل إلى ثلاثة فاصلة أربعة وخمسين بانحراف معياري قدره واحد فاصلة مئتان وثلاثة وثمانون؛ وهي قيمة تعكس توافقاً أفضل نسبياً مقارنة بفقرات أخرى؛ فالغالبية العظمى التي تبلغ اثنين وستين فاصلة أربعة بالمئة تتفق على أن الهدف الأسعى للأمن السيبراني هو ديمومة الخدمات؛ فالموظف الحكومي يدرك أن انقطاع الأنظمة يعني توقف مصالح المواطنين؛ فـ خيار "أوافق" تصدر بنسبة ستة وثلاثين فاصلة خمسة بالمئة؛ وهذا الوعي يربط بين الأمن السيبراني وبين الكفاءة التشغيلية للمنظمة؛ فربما يتم النظر للأمن كعامل تمكين للأعمال وليس كعائق إجرائي؛ والبيانات توضح أن نسبة المعارضين لهذا الطرح قليلة نسبياً مقارنة بفقرات سابقة؛ فالتوافق حول مفهوم استمرارية الأعمال يبدو أكثر رسوخاً في الثقافة المؤسسية؛ فالمحايدون يشكلون اثني عشر فاصلة اثنين بالمئة؛ ولعل ذلك يرجع لعدم تماسك الخطط البديلة (Disaster Recovery) في بعض الجهات؛ فالموظف الذي لم يختبر خطة طوارئ ناجحة قد يتردد في الموافقة؛ فالانحراف المعياري الأقل هنا يوحي بأن هناك إجماعاً أكبر على النتائج الملموسة للاستراتيجيات؛ فالحفاظ على سمعة الجهة الحكومية وخدماتها الرقمية هو المحرك الأساسي للاقتناع بهذه السياسات؛ والارتباط بين الأمن والاستمرارية يعد مفهماً جوهرياً في رؤية المملكة ألفين وثلاثين؛

فالحكومة الرقمية تتطلب توفراً دائماً للخدمات: وهذه النتائج تدعم التوجه نحو الاستثمار في أنظمة النسخ الاحتياطي والحلول السحابية الآمنة؛ فالثقة الإحصائية هنا تمنح القيادات مبرراً قوياً لتخصيص موارد أكبر لضمان عدم التوقف؛ فالموظفون يرون الأثر المباشر للأمن على استقرار وظائفهم وخدماتهم؛ والبيئة الرقمية المستقرة هي الثمرة الحقيقية التي يقطفها الجميع من تطبيق هذه الاستراتيجيات بفعالية واحترافية عالية.

جدول 9: التحليل الإحصائي لمساعدة استراتيجيات الأمن السيبراني في ضمان استمرارية الأعمال والخدمات الحكومية.

تساعد استراتيجيات الأمن السيبراني في ضمان استمرارية الأعمال والخدمات الحكومية.					
	Frequency	Percent	Valid Percent	Cumulative Percent	
أوافق	96	36,5	36,5	36,5	Valid
أوافق بشدة	68	25,9	25,9	62,4	
لا أوافق	43	16,3	16,3	78,7	
محايد	32	12,2	12,2	90,9	
لا أوافق بشدة	24	9,1	9,1	100,0	
Total	263	100,0	100,0		



شكل توضيحي 8: التمثيل البياني لمساعدة استراتيجيات الأمن السيبراني في ضمان استمرارية الأعمال والخدمات الحكومية.

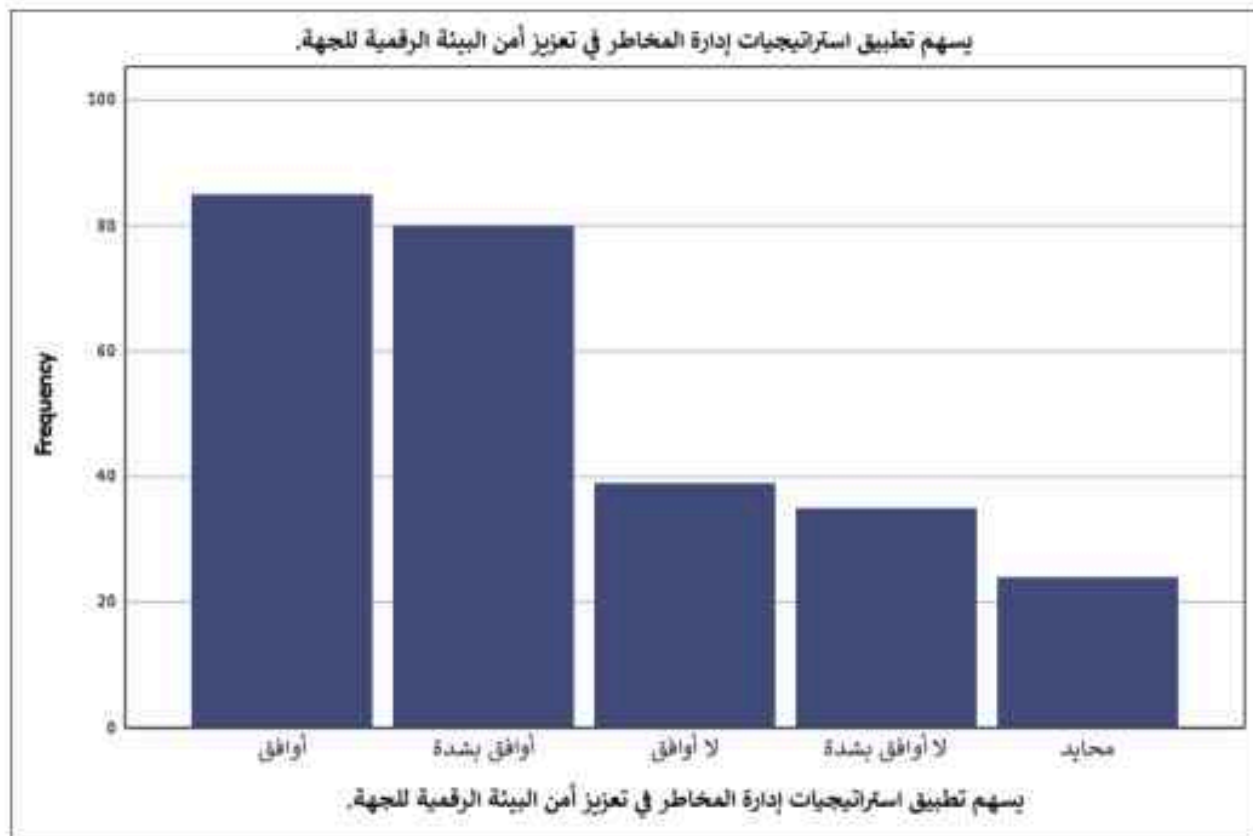
• يسهم تطبيق استراتيجيات إدارة المخاطر في تعزيز أمن البيئة الرقمية للجهة.

يظهر المتوسط الحسابي البالغ ثلاثة فاصلة اثنين وخمسين قناعة راسخة بأثر إدارة المخاطر على سلامة المحيط التقني؛ فالموافقون والموافقون بشدة يمثلون اثنين وستين فاصلة سبعة بالمئة من مجمل العينة؛ وهو ما يعزز فكرة أن الأمن السيبراني ليس مجرد جدران نارية بل هو نتاج لعملية إدارة مخاطر واعية؛ فالبيئة الرقمية الآمنة تحتمل وجود سياسات تحد من التصرفات البشرية الخاطئة وتحمي الأصول التقنية؛ وربما يفسر الانحراف المعياري البالغ واحد فاصلة أربعة مئة تفاوت مستويات الأمان بين الإدارات المختلفة داخل الجهة الواحدة؛ فالموظف في قطاع العمليات قد يشعر بأمان أكثر من موظف في قطاع التعاملات الخارجية؛ والبيانات تكشف أن نسبة غير الموافقين (لا أوافق ولا أوافق بشدة) تصل إلى ثمانية وعشرين بالمئة؛ ولعل هذا يعود إلى وجود ثغرات أمنية ملاحظة أو ضعف في الرقابة الرقمية في بعض الجوانب؛ فالشعور بالأمن هو شعور تراكمي يبني من خلال خلو بيئة العمل من الحوادث المنقصة؛ فالمحايدون الذين بلغت نسبتهم تسعة فاصلة واحد بالمئة قد يكونون ممن لا يملكون صلاحيات تقنية واسعة تمكنهم من الحكم على أمن البيئة الرقمية؛ والنتائج في مجملها تشير إلى اتجاه إيجابي يربط بين الفكر الاستراتيجي والواقع التقني؛ فتعزيز الأمن يتطلب تحويل الاستراتيجية إلى ممارسات يومية يعيشها الموظف؛

والقيمة المرتفعة للمتوسط تعكس نجاحاً نسبياً في غرس هذه القيمة داخل المؤسسة: فالحماية الرقمية أصبحت مطلباً ملجأً في ظل تزايد الهجمات السيبرانية العالمية؛ وهذا التوزيع التكراري يدفع نحو مزيد من الرقابة والتدقيق لضمان أن كل موظف يشعر فعلياً بحماية المنظومة لبياناته وأدوات عمله؛ فالبينة الآمنة هي المحفز الأول للإبداع الرقمي في القطاع الحكومي.

جدول 10: التحليل الإحصائي لمساهمة تطبيق استراتيجيات إدارة المخاطر في تعزيز أمن البيئة الرقمية للجهة.

يسهم تطبيق استراتيجيات إدارة المخاطر في تعزيز أمن البيئة الرقمية للجهة.					
	Frequency	Percent	Valid Percent	Cumulative Percent	
أوافق	٨٥	٣٢,٣	٣٢,٣	٣٢,٣	Valid
أوافق بشدة	٨٠	٣٠,٤	٣٠,٤	٦٢,٧	
لا أوافق	٣٩	١٤,٨	١٤,٨	٧٧,٦	
لا أوافق بشدة	٣٥	١٣,٣	١٣,٣	٩٠,٩	
محايد	٢٤	٩,١	٩,١	١٠٠,٠	
Total	٢٦٣	١٠٠,٠	١٠٠,٠		



شكل توضيحي 9 : التمثيل البياني لمساهمة تطبيق استراتيجيات إدارة المخاطر في تعزيز أمن البيئة الرقمية للجهة.

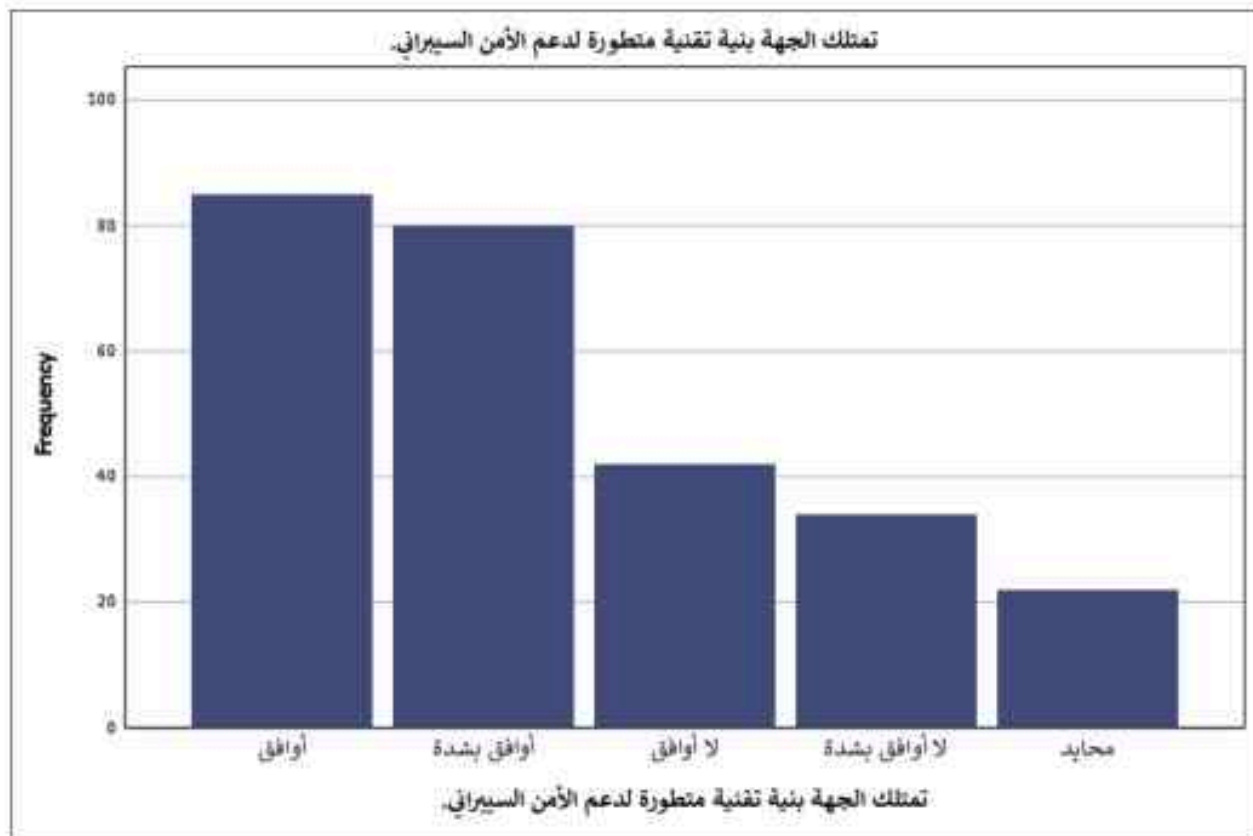
• تمتلك الجهة بنية تقنية متطورة لدعم الأمن السيبراني.

يستقر المتوسط الحسابي لهذه الفقرة عند ثلاثة فاصلة واحد وخمسين مع انحراف معياري قدره واحد فاصلة أربعة مئة؛ مما يشير إلى وجود رضا عام يتخلله تباين في تقييم جودة العتاد التقني؛ فالموافقون والموافقون بشدة يشكلون اثنين وستين فاصلة سبعة بالمئة؛ وهي نسبة تعكس حجم الإنفاق الحكومي الضخم على البنية التحتية المعلوماتية؛ فالمستجيبون يشعرون بامتلاكهم أدوات تقنية حديثة؛ غير أن ثمانية وعشرين فاصلة تسعة بالمئة عبروا عن عدم موافقتهم؛ فربما يعاني هؤلاء من أجهزة قديمة أو برمجيات غير محدثة في مكاتهم؛ فالنظور التقني قد لا يشمل كافة الفروع أو الإدارات بنفس المستوى؛ فالبنية المتطورة تتطلب تحديثاً شاملاً لا يستثني أحداً؛ فالانحراف المعياري المرتفع يبرهن على أن "التطور" مفهوم نسبي يختلف باختلاف ما يتوفر للموظف من إمكانيات؛ ولعل نسبة الجياد المنخفضة ثمانية فاصلة أربعة بالمئة توحي بأن الموظفين لديهم رأي قاطع في هذه المسألة؛ فالجهاز والشبكة هما أدوات العمل اليومية التي يسهل الحكم عليها؛ وتظهر النتائج أن هناك حاجة لسد الفجوة التقنية بين الإدارات المتقدمة وتلك التي لا تزال تعتمد على نظم تقليدية؛ فالبنية التقنية هي العمود الفقري الذي يستند إليه الأمن السيبراني؛ وأي ضعف في هذا الجانب سيؤدي حتماً لفشل الاستراتيجيات مهما كانت محكمة؛ فالقيمة الإحصائية هنا تشجع

على الاستمرار في عمليات الإحلال والتبديل للأنظمة المتهاككة؛ فالمواكبة التقنية هي السبيل الوحيد لمواجهة تهديدات الجيل الخامس وما بعدها؛ والرضا العام المسجل يمنح انطباعاً بأن المملكة تسير في الطريق الصحيح نحو بناء حصون رقمية منيعة؛ فالبنية التحتية هي الاستثمار الحقيقي في اقتصاد المعرفة والأمن الوطني.

جدول ١١ : التحليل الإحصائي لامتلاك الجهة بنية تقنية متطورة تدعم الأمن السيبراني.

تمتلك الجهة بنية تقنية متطورة تدعم الأمن السيبراني.					
	Frequency	Percent	Valid Percent	Cumulative Percent	
أوافق	٨٥	٣٢,٣	٣٢,٣	٣٢,٣	Valid
أوافق بشدة	٨٠	٣٠,٤	٣٠,٤	٦٢,٧	
لا أوافق	٤٢	١٦,٠	١٦,٠	٧٨,٧	
لا أوافق بشدة	٣٤	١٢,٩	١٢,٩	٩١,٦	
محايد	٢٢	٨,٤	٨,٤	١٠٠,٠	
Total	٢٦٣	١٠٠,٠	١٠٠,٠		



شكل توضيحي 10 : التمثيل البياني لامتلاك الجهة بنية تقنية متطورة لدعم الأمن السيبراني.

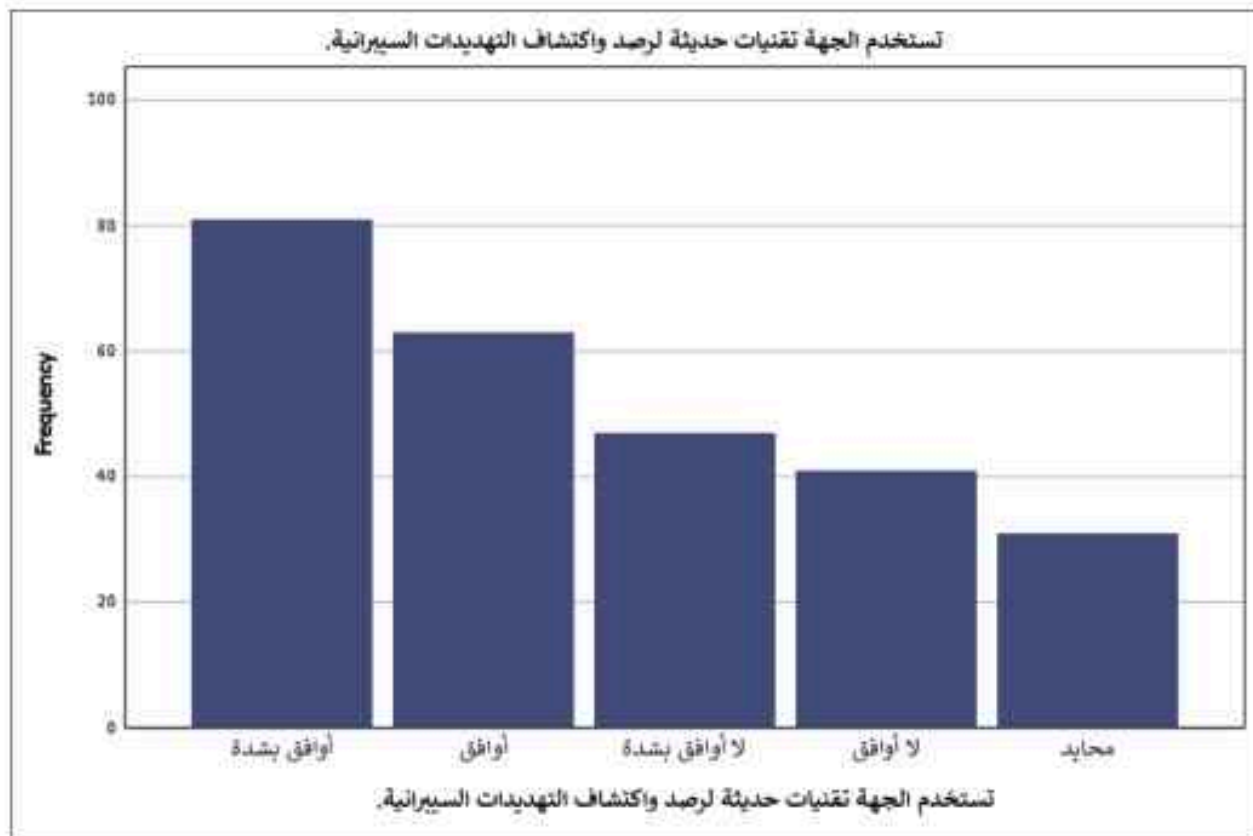
• تستخدم الجهة تقنيات حديثة لرصد واكتشاف التهديدات السيبرانية.

تسجل هذه الفقرة متوسطاً حسابياً هو الأقل في هذه المجموعة بواقع ثلاثة فاصلة أربعة وثلاثين؛ مع انحراف معياري مرتفع نسبياً قدره واحد فاصلة أربعة مئة وخمسة وتسعون؛ وهذا الرقم يعكس حالة من القلق الإحصائي أو عدم الرضا الكامل عن أدوات الرصد؛ فالموافقون بشدة والموافقون يمثلون أربعة وخمسين فاصلة ثمانية بالمئة فقط؛ وهي نسبة أقل من نظيراتها في الفقرات السابقة؛ فربما يشعر الموظفون بأن أدوات الرصد الحالية ليست بالمستوى المطلوب لمواجهة التهديدات المتطورة؛ أو قد يكون هناك نقص في الشفافية فيما يخص عمليات الرصد التي تقوم بها إدارات أمن المعلومات؛ فالبيانات تظهر أن نسبة عدم الموافقة (بشدة وبدونها) تصل إلى ثلاثة وثلاثين فاصلة خمسة بالمئة؛ وهي كتلة كبيرة لا يمكن تجاهلها؛ ولعل السبب يكمن في وقوع حوادث أمنية لم تكتشفها الأنظمة إلا بعد فوات الأوان؛ فعملية الرصد تتطلب تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة التي قد لا تتوفر للجميع؛ فالمحايدون بنسبة أحد عشر فاصلة ثمانية بالمئة ربما يفتقرون للمعرفة التقنية بما يدور في مراكز العمليات الأمنية (SOC)؛ فالانحراف المعياري القريب من الواحد والنصف يشي بوجود فجوة كبيرة في التجربة التقنية بين المستجيبين؛ فمنهم من يرى أنظمة عالمية ومنهم من يرى غياباً تاماً لأدوات الرصد؛ والنتائج تدق ناقوس الخطر

بضرورة تعزيز قدرات الاكتشاف المبكر: فالأمن لا يقتصر على الحماية بل يمتد لسرعة الرصد؛ وهذا المتوسط المندني نسبياً يستوجب مراجعة العقود التقنية وتحديث منصات الرقابة الأمنية: فالثقة في قدرة المنظمة على اكتشاف الاختراق هي جزء من الاستقرار النفسي والمهني للموظف؛ والارتقاء بهذا الرقم يتطلب استثمارات ذكية في برمجيات الرصد التلقائي والاستباق.

جدول 12: التحليل الإحصائي لاستخدام الحية تقنيات حديثة لرصد واكتشاف التهديدات السيبرانية.

تستخدم الجهة تقنيات حديثة لرصد واكتشاف التهديدات السيبرانية.					
	Frequency	Percent	Valid Percent	Cumulative Percent	
أوافق بشدة	٨١	٣٠,٨	٣٠,٨	٣٠,٨	Valid
أوافق	٦٣	٢٤,٠	٢٤,٠	٥٤,٨	
لا أوافق بشدة	٤٧	١٧,٩	١٧,٩	٧٢,٦	
لا أوافق	٤١	١٥,٦	١٥,٦	٨٨,٢	
محايد	٣١	١١,٨	١١,٨	١٠٠,٠	
Total	٢٦٣	١٠٠,٠	١٠٠,٠		



شكل لوضيحي 11: النمط السائد لاستخدام الجهة تقنيات حديثة لرصد واكتشاف التهديدات السيبرانية.

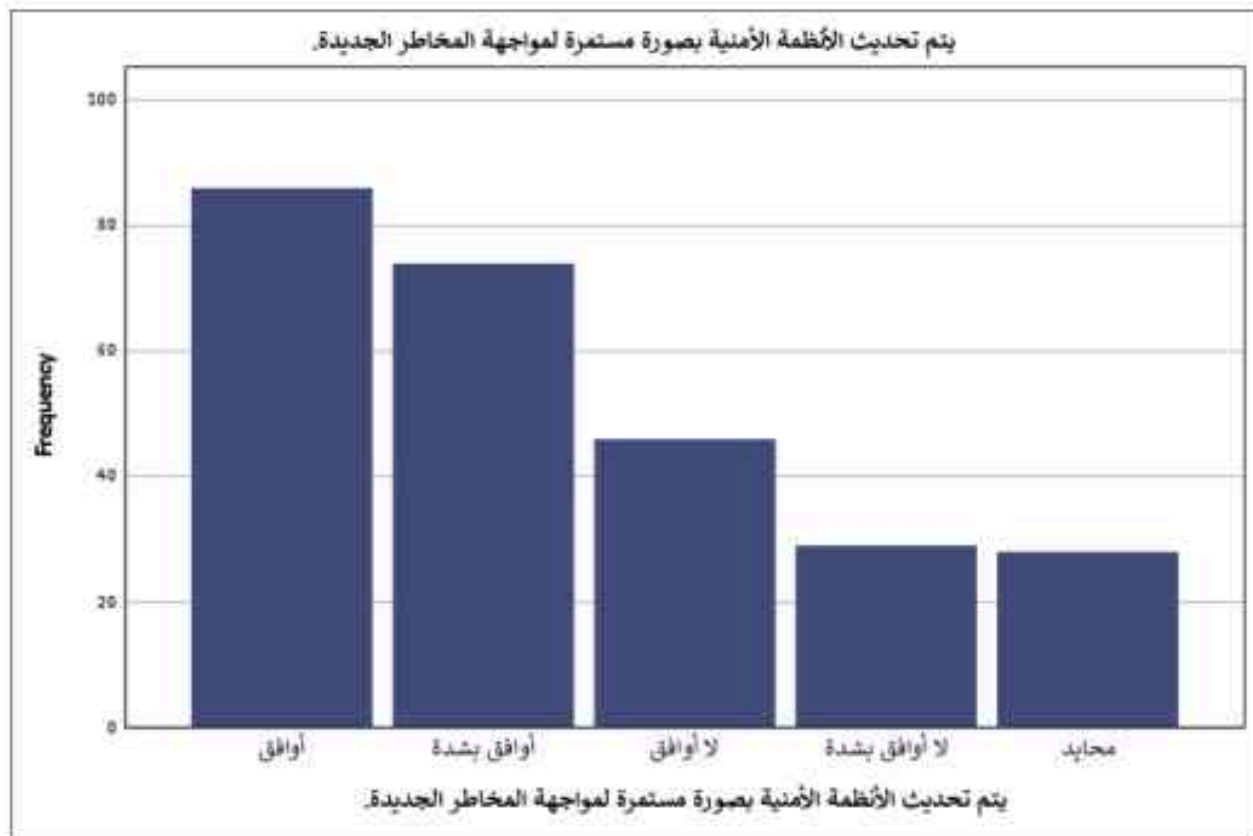
• يتم تحديث الأنظمة الأمنية بصورة مستمرة لمواجهة المخاطر الجديدة.

تتحصل عملية التحديث المستمر على متوسط ثلاثة فاصلة تسعة وأربعين؛ وهو رقم جيد يشير إلى وعي بأهمية الملاحقة الزمنية للتهديدات؛ فالموافقون والموافقون بشدة يشكلون ستين فاصلة ثمانية بالمئة من العينة؛ وهذا التوجه يتماشى مع أفضل الممارسات العالمية في إدارة الرفق الأمنية (Patch Management)؛ فالتحديث ليس رفاهية بل ضرورة للبقاء؛ وربما يفسر الانحراف المعياري البالغ واحد فاصلة ثلاثمائة وثلاثة وخمسين تفاوت سرعة الاستجابة للتحديثات بين الأنظمة المختلفة؛ فالأنظمة التشغيلية الأساسية قد تحظى بالأولوية بينما تظل أنظمة فرعية عرضة للمخاطر؛ والبيانات تظهر أن ثمانية وعشرين فاصلة خمسة بالمئة لا يوافقون على كفاية التحديثات؛ ولعل هذا الشعور ناتج عن بطء الإجراءات الإدارية في اعتماد التحديثات الجديدة خوفاً من تأثيرها على استقرار العمل؛ فالموازنة بين الأمان والاستمرارية تمثل تحدياً دائماً؛ ففئة المحايدين البالغة عشرة فاصلة ستة بالمئة تعكس شريحة من الموظفين لا تدرك حجم العمليات التي تتم في الخلفية لتحديث الأنظمة؛ فالنتائج في مجملها إيجابية وتدعم فكرة أن التحديث جزء من الثقافة التقنية للجهة؛ غير أن الوصول إلى مستويات أمان عليا يتطلب تقليل نسبة المعارضين من خلال الأتمتة الكاملة لعمليات التحديث؛ فالاعتماد على التدخل البشري قد يؤدي إلى تأخيرات غير محسوبة؛ والارتباط بين

التحديث المستمر وتقليل المخاطر ارتباط عضوي تؤكد القراءات الإحصائية: فالموظفون يثقون في التحديث كدرع واقٍ: وهذا الرضا النسبي يمنح الإدارة حافزاً لتطوير آليات التحديث لتصبح أكثر سلاسة وشمولية لكافة الأصول الرقمية دون استثناء؛ فالتحديث المستمر هو الضمانة الوحيدة لمواجهة تهديدات "يوم الصفر".

جدول 13 - التحليل الإحصائي لتحديث الأنظمة الأمنية بصورة مستمرة لمواجهة المخاطر الجديدة.

يتم تحديث الأنظمة الأمنية بصورة مستمرة لمواجهة المخاطر الجديدة.					
Cumulative Percent	Valid Percent	Percent	Frequency		
٣٢,٧	٣٢,٧	٣٢,٧	٨٦	أوافق	Valid
٦٠,٨	٤٨,١	٤٨,١	٧٤	أوافق بشدة	
٧٨,٣	١٧,٥	١٧,٥	٤٦	لا أوافق	
٨٩,٤	١١,٠	١١,٠	٢٩	لا أوافق بشدة	
١٠٠,٠	١٠,٦	١٠,٦	٢٨	محايد	
	١٠٠,٠	١٠٠,٠	٢٦٣	Total	



شكل 12: التمثيل البياني لتحديث الأنظمة الأمنية بصورة مستمرة لمواجهة المخاطر الجديدة.

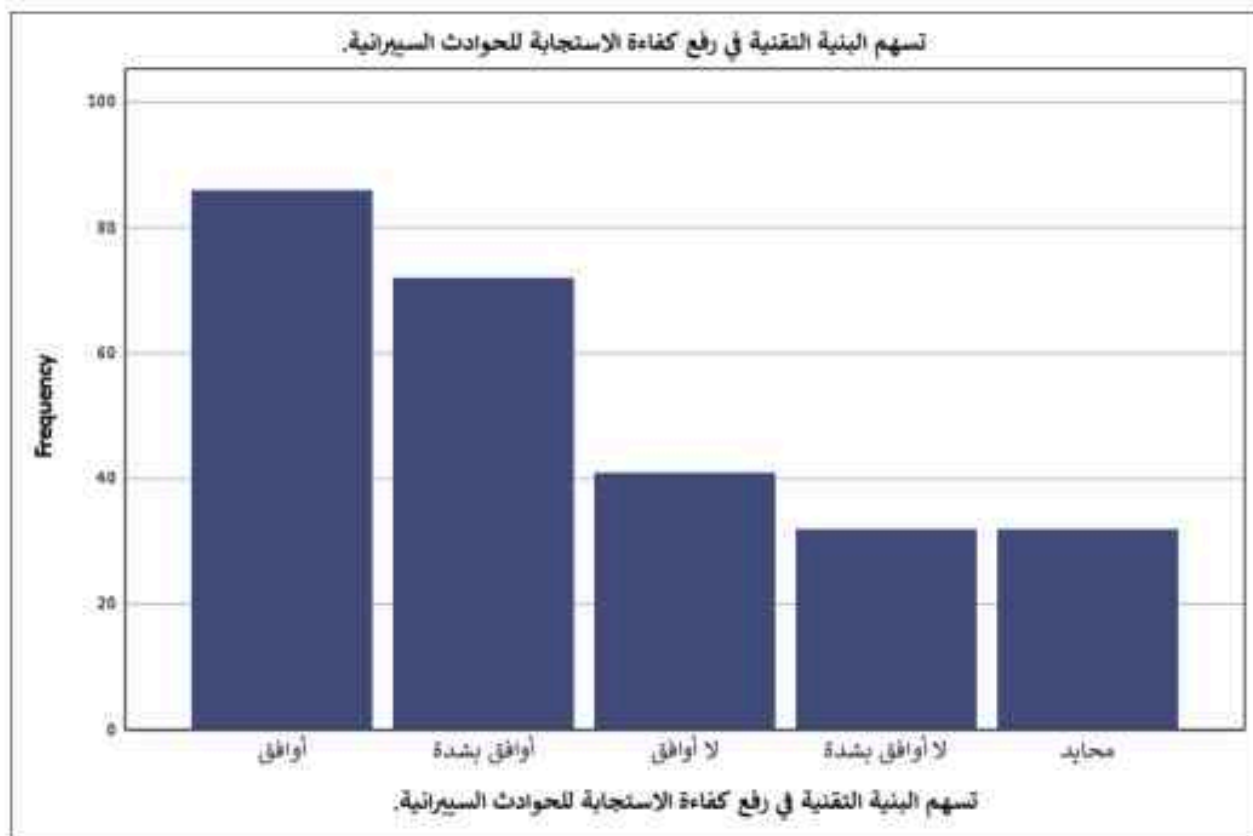
• تسهم البنية التقنية في رفع كفاءة الاستجابة للحوادث السيبرانية.

يسجل المتوسط الحسابي لهذه الفقرة ثلاثة فاصلة ثمانية وأربعين: مع انحراف معياري قدره واحد فاصلة ثلاثمائة وتسعة وخمسون؛ مما يعطي انطباعاً بوجود علاقة إيجابية بين جودة العتاد وسرعة معالجة الأزمات؛ فالموافقون والموافقون بشدة يمثلون ستين فاصلة واحد بالمئة من العينة؛ وهذا يشير إلى أن الاستثمار في البنية التحتية لم يكن مجرد مظهر تقني بل كان له أثر إجرائي ملموس؛ فكفاءة الاستجابة تتطلب أدوات تحليلية وسرعات ربط عالية وقدرات تخزينية ضخمة؛ وربما يرجع عدم موافقة سبعة وعشرين فاصلة ثمانية بالمئة إلى تجارب سابقة اتسمت بالبطء في التعامل مع حوادث معينة؛ فالبنية التقنية وحدها لا تكفي إذا غابت التنسيقات الإدارية؛ فالتنشتت في الآراء يلمح إلى أن الكفاءة ليست موحدة في جميع مراكز الاستجابة التابعة للجهة؛ فالمحايدون بنسبة اثني عشر فاصلة اثنين بالمئة قد يكونون ممن لم يشاركوا قط في التعامل مع حادث سيبراني؛ فالنتائج تؤكد أن البنية القوية هي الممكن الأساسي لفرق الطوارئ الأمنية (CERT)؛ فالارتقاء بهذا المتوسط يتطلب دمج الأنظمة التقنية بروتوكولات استجابة واضحة ومجربة؛ فالمستجيبون يربطون بين توفر التقنية وبين النجاح في احتواء الأزمات؛ وهذه القراءة الإحصائية تعزز التوجه نحو بناء غرف عمليات أمنية متطورة؛ فالتكنولوجيا هي المضاعف الحقيقي للجهد البشري في

أوقات الأزمات؛ والميل نحو الموافقة بمنح المصادقية لخطط التطوير التقني الحالية؛ فالبنية التحتية ليست مجرد تكلفة بل هي دُخر استراتيجي يظهر معدنه عند وقوع الخطر؛ والبيانات تدعو لمزيد من التدريبات المحاكية للحوادث لاختبار مدى كفاءة هذه البنية في ظروف ضغط حقيقية.

جدول 14: التحليل الإحصائي لمساهمة البنية التقنية في رفع كفاءة الاستجابة للحوادث السيبرانية.

تسهم البنية التقنية في رفع كفاءة الاستجابة للحوادث السيبرانية.					
Cumulative Percent	Valid Percent	Percent	Frequency		
٣٢,٧	٣٢,٧	٣٢,٧	٨٦	أوافق	Valid
٦٠,١	٢٧,٤	٢٧,٤	٧٢	أوافق بشدة	
٧٥,٧	١٥,٦	١٥,٦	٤١	لا أوافق	
٨٧,٨	١٢,٢	١٢,٢	٣٢	لا أوافق بشدة	
١٠٠,٠	١٢,٢	١٢,٢	٣٢	محايد	
	١٠٠,٠	١٠٠,٠	٢٦٣	Total	



شكل توضيحي 13: التمثيل البياني لمساهمة البنية التقنية في رفع كفاءة الاستجابة للحوادث السيبرانية.

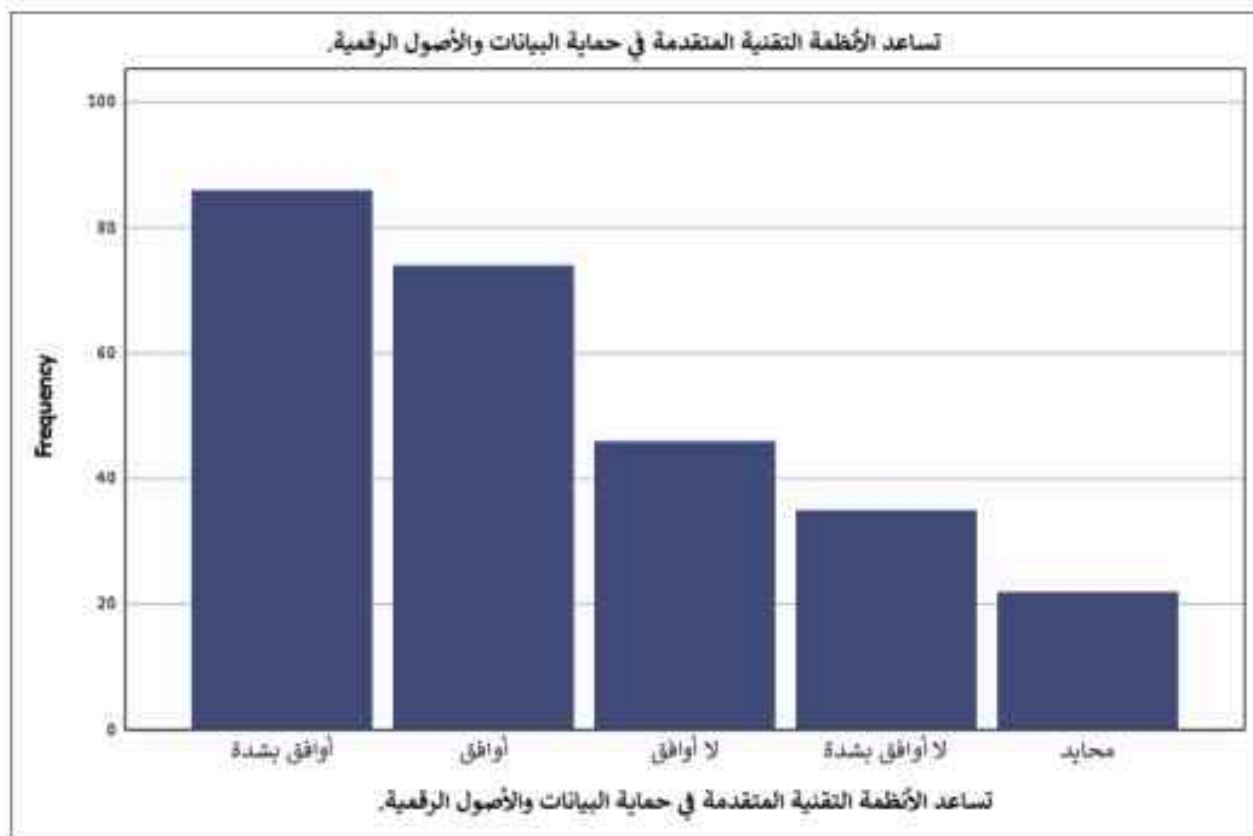
• تساعد الأنظمة التقنية المتقدمة في حماية البيانات والأصول الرقمية.

يصل المتوسط الحسابي هنا إلى ثلاثة فاصلة تسعة وأربعين؛ وهو ما يضع الأنظمة المتقدمة في مرتبة عالية من حيث الأهمية المدركة؛ فخيار "أوافق بشدة" تصدر بنسبة اثنين وثلاثين فاصلة سبعة بالمئة؛ بينما وافق ثمانية وعشرون فاصلة واحد بالمئة؛ فالإجماع الإيجابي يتجاوز الستين بالمئة؛ وهذا يعكس ثقة الموظفين في أن التكنولوجيا هي الحارس الأمين لبياناتهم؛ فالتشفير وأنظمة منع تسريب البيانات (DLP) أصبحت أدوات أساسية لا غنى عنها؛ وربما يفسر الانحراف المعياري البالغ واحد فاصلة أربع مئة وخمسة وثلاثين وجود مخاوف لدى ثلاثين بالمئة تقريباً من المشاركين حول مدى كفاءة هذه الأنظمة؛ فالهجمات السيبرانية المعاصرة قادرة أحياناً على تجاوز أكثر الأنظمة تعقيداً؛ فالتشتت في الآراء يوحي بأن الحماية ليست مطلقة في نظر الجميع؛ فالمحايدون بنسبة ثمانية فاصلة أربعة بالمئة يمثلون فئة قد لا تتعامل مع بيانات حساسة بشكل مباشر؛ فالنتائج تبرز أهمية الجمع بين التقدم التقني والوعي البشري؛ فحماية البيانات هي مسؤولية مشتركة وليست مجرد إعدادات برمجية؛ والقيمة المرتفعة للمتوسط تعطي دفعة لصناع القرار للاستثمار في تقنيات حماية البيانات السيادية؛ فالمواطنون والموظفون يتوقعون أعلى مستويات الخصوصية والأمان؛ وهذا الرقم الإحصائي يعزز من مكانة الأمن السيبراني كأولوية قصوى؛ فالأنظمة المتقدمة

تحتمل مستقبلاً أكثر أماناً إذا ما تمت إدارتها بكفاءة عالية؛ والرضا العام المسجل يبرهن على نجاح الاستراتيجيات التقنية في خلق بيئة رقمية موثوقة؛ فالحماية هي القيمة المضافة التي تقدمها التكنولوجيا للمجتمع الحكومي في ظل التحول الرقمي الشامل.

جدول 15: التطوير الإحصائي لمساعدة الأنظمة التقنية المتقدمة في حماية البيانات والأصول الرقمية.

تساعد الأنظمة التقنية المتقدمة في حماية البيانات والأصول الرقمية.					
Cumulative Percent	Valid Percent	Percent	Frequency		
٣٢,٧	٣٢,٧	٣٢,٧	٨٦	أوافق بشدة	Valid
٦٠,٨	٤٨,١	٤٨,١	٧٤	أوافق	
٧٨,٣	١٧,٥	١٧,٥	٤٦	لا أوافق	
٩١,٦	١٣,٣	١٣,٣	٣٥	لا أوافق بشدة	
١٠٠,٠	٨,٤	٨,٤	٢٢	محايد	
	١٠٠,٠	١٠٠,٠	٢٦٣	Total	



شكل توضيحي 14: التمثيل البياني لمساعدة الأنظمة التقنية المتقدمة في حماية البيانات والأصول الرقمية.

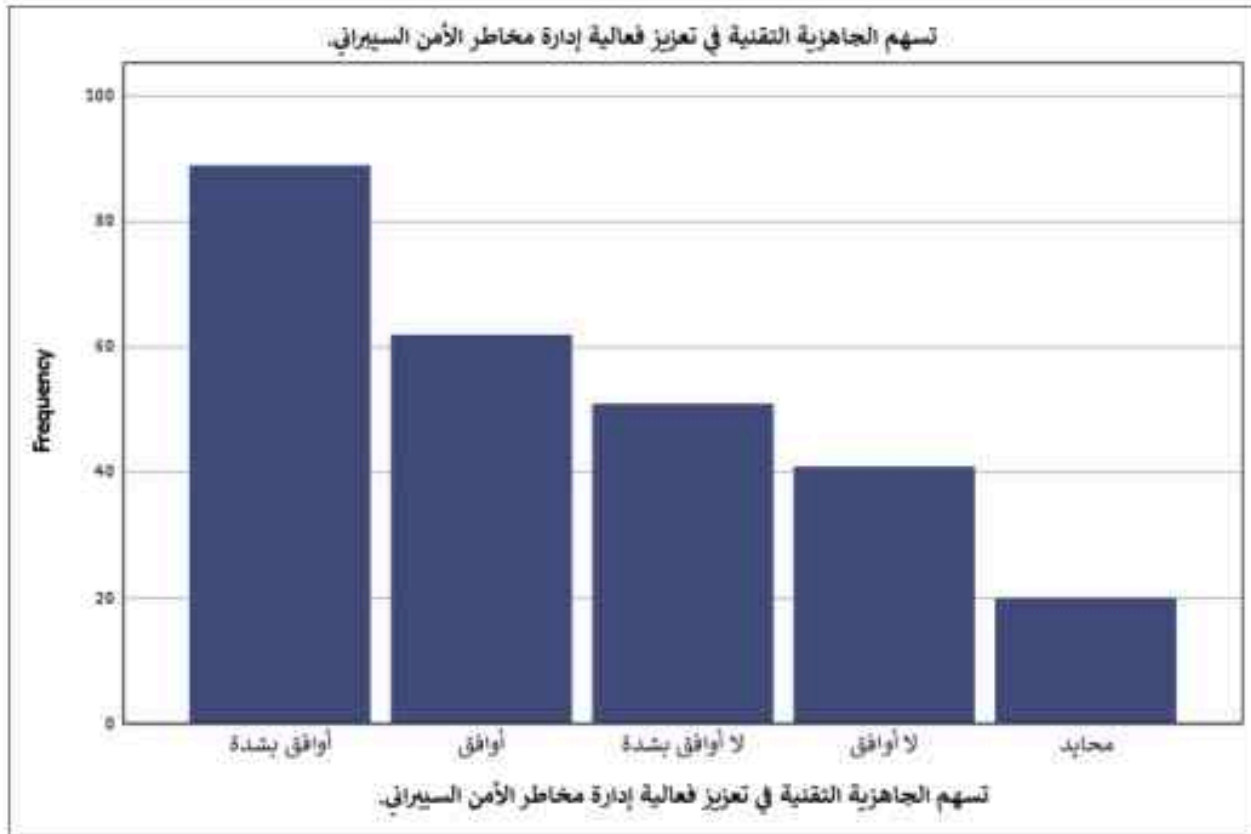
• تسهم الجاهزية التقنية في تعزيز فعالية إدارة مخاطر الأمن السيبراني.

تحصلت هذه الفقرة على متوسط ثلاثة فاصلة سبعة وثلاثين؛ وهو رقم يميل للموافقة لكنه يحمل في طياته أكبر قدر من التشتت في هذه المجموعة؛ فالانحراف المعياري سجل أعلى قيمة بواقع واحد فاصلة خمسمئة وسبعة وأربعين؛ وهذا التباين الحاد يشير إلى اختلاف جذري في فهم معنى "الجاهزية" بين الموظفين؛ فبينما وافق سبعة وخمسون فاصلة أربعة بالمئة على هذا الدور؛ نجد أن خمسة وثلاثين بالمئة عارضوا ذلك بشدة أو بوضوح؛ فالفجوة واسعة جداً وتوحي بأن الجاهزية في بعض القطاعات قد تكون مجرد شعارات لا رصيد لها في الواقع؛ فربما تفتقر الجهة إلى سيناريوهات الاختبار الحقيقي لجاهزيتها؛ فالموظف الذي يرى ضعفاً في التجهيزات لا يمكنه الاقتناع بفعالية إدارة المخاطر؛ فالمحايدون بنسبة سبعة فاصلة ستة بالمئة هم الأقل عدداً؛ مما يعني أن القضية جدلية وتثير آراء قاطعة؛ فالنتائج تستدعي مراجعة شاملة لمفهوم الجاهزية وتحويله من مجرد امتلاك أجهزة إلى امتلاك قدرة حقيقية على المواجهة؛ فالفشل في اختبارات الجاهزية قد يؤدي إلى انهيار منظومة الأمن بالكامل؛ والارتباط الإحصائي بين الجاهزية والفعالية ارتباط وثيق؛ فبدون أدوات جاهزة تظل الاستراتيجيات مجرد أحلام؛ وهذا المتوسط المنخفض نسبياً مقارنة بغيره يضع المسؤولين أمام مسؤولية تحديث العناد وتدريب الكوادر على استخدامه تحت

الضغط؛ فمن المحتمل أن يكون نقص الموارد في بعض الإدارات هو السبب خلف هذا التقييم المنخفض: فالجاهزية هي الاختبار الحقيقي لصدق النوايا الاستراتيجية؛ وهذه القراءات تدعو لتبني معايير قياس دقيقة للجاهزية التقنية تتجاوز مجرد الحصر الكمي للأجهزة والبرامج.

جدول 16 - التحليل الإحصائي لمساهمة الجاهزية التقنية في تعزيز فعالية إدارة مخاطر الأمن السيبراني.

تسهم الجاهزية التقنية في تعزيز فعالية إدارة مخاطر الأمن السيبراني.					
	Frequency	Percent	Valid Percent	Cumulative Percent	
أوافق بشدة	٨٩	٣٣,٨	٣٣,٨	٣٣,٨	Valid
أوافق	٦٢	٢٣,٦	٢٣,٦	٥٧,٤	
لا أوافق بشدة	٥١	١٩,٤	١٩,٤	٧٦,٨	
لا أوافق	٤١	١٥,٦	١٥,٦	٩٢,٤	
محايد	٢٠	٧,٦	٧,٦	١٠٠,٠	
Total	٢٦٣	١٠٠,٠	١٠٠,٠		



شكل توضيحي 15 : التمثيل البياني لمساهمة الجاهزية التقنية في تعزيز فعالية إدارة مخاطر الأمن السيبراني.

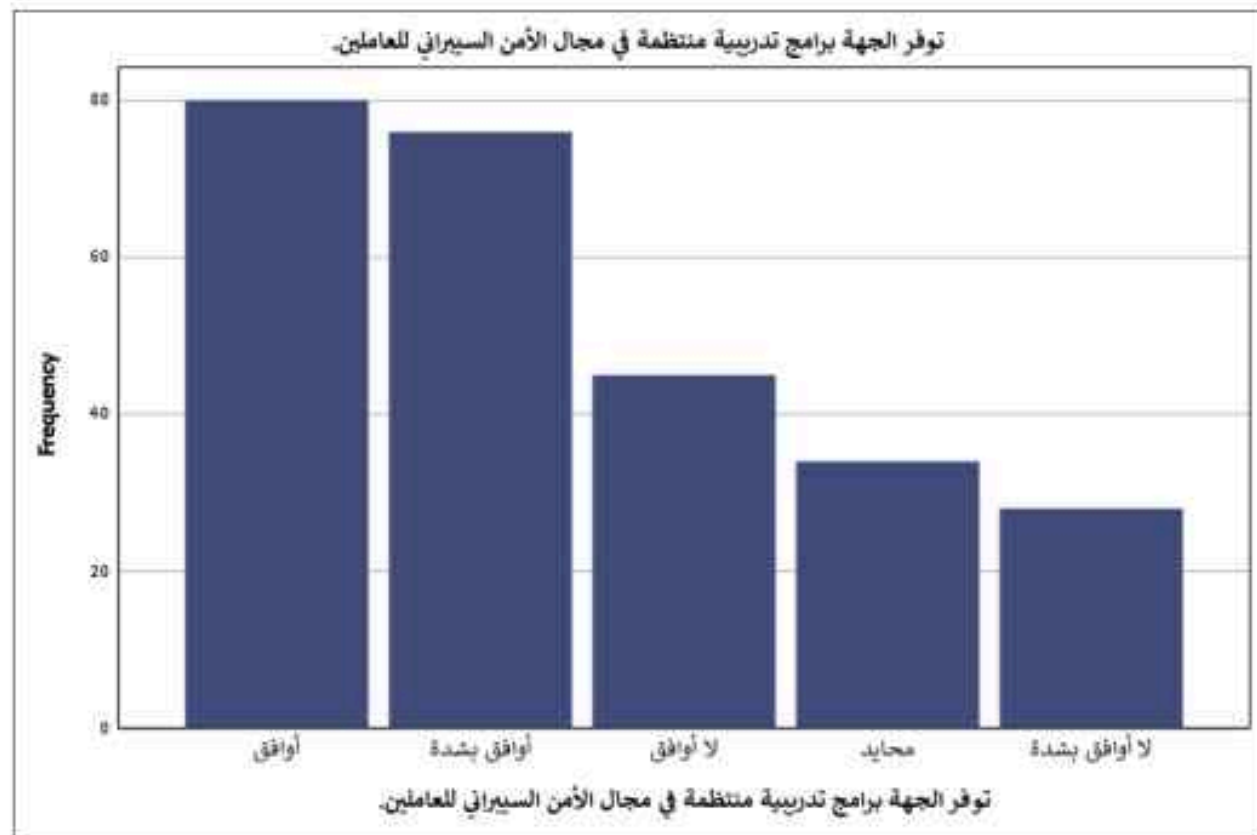
• توفر الجهة برامج تدريبية منتظمة في مجال الأمن السيبراني للعاملين.

يستقر المتوسط الحسابي للتدريب عند ثلاثة فاصلة خمسين؛ مع انحراف معياري قدره واحد فاصلة ثلاثمائة وثمانية وأربعون؛ مما يشير إلى وجود جهد تدريبي ملموس يظال غالبية الموظفين؛ فالموافقون والموافقون بشدة يشكلون تسعة وخمسين فاصلة ثلاثة بالمئة؛ وهذا يعكس إدراك الجهة أن العنصر البشري هو الحلقة الأضعف والأقوى في آن واحد؛ فالاستثمار في العقول يوازي الاستثمار في الأنظمة؛ وربما يرجع عدم موافقة سبعة وعشرين فاصلة سبعة بالمئة إلى ندرة الدورات في بعض التخصصات أو عدم شمولية التدريب لكافة المستويات الوظيفية؛ فالتدريب المنتظم يتطلب استدامة في الميزانيات وتطويراً في المحتوى التدريبي؛ فالمحايدون بنسبة اثني عشر فاصلة تسعة بالمئة قد يكونون ممن لم تصله دعوات التدريب بعد؛ فالنتائج تبرهن على أن هناك حراكاً توعوياً جيداً لكنه يحتاج لمزيد من التنظيم؛ فالانحراف المعياري يشير إلى أن تجربة التدريب ليست متساوية بين الجميع؛ فممن من يحصل على دورات عالمية وممن من يكتفي بورش عمل بسيطة؛ والارتباط بين التدريب والفعالية الأمنية هو حجر الزاوية في بناء الثقافة الوقائية؛ فالموظف المدرب هو خط الدفاع الأول ضد التصيد الاحتيالي والهندسة الاجتماعية؛ وهذا المتوسط المشجع يمنح الإدارة دافعاً لتبني منصات تدريبية مستمرة ذاتية التعلم؛ فالأمن السيبراني يتغير بسرعة تتطلب تعلماً

يوميًا وليس مجرد دورة سنوية؛ والرضا العام المسجل يمنح شرعية لخطط التطوير البشري؛ فالتدريب هو الأداة التي تحول السياسات الأمنية من نصوص صماء إلى ممارسات حية في وجدان الموظف وسلوكه المهني اليومي.

جدول 17: التحليل الإحصائي لتوفر الجهة برامج تدريبية منتظمة في مجال الأمن السيبراني للعاملين.

توفر الجهة برامج تدريبية منتظمة في مجال الأمن السيبراني للعاملين.					
	Cumulative Percent	Valid Percent	Percent	Frequency	
Valid	30,4	30,4	30,4	80	أوافق
	59,3	28,9	28,9	76	أوافق بشدة
	76,4	17,1	17,1	45	لا أوافق
	89,4	12,9	12,9	34	محايد
	100,0	10,6	10,6	28	لا أوافق بشدة
		100,0	100,0	263	Total



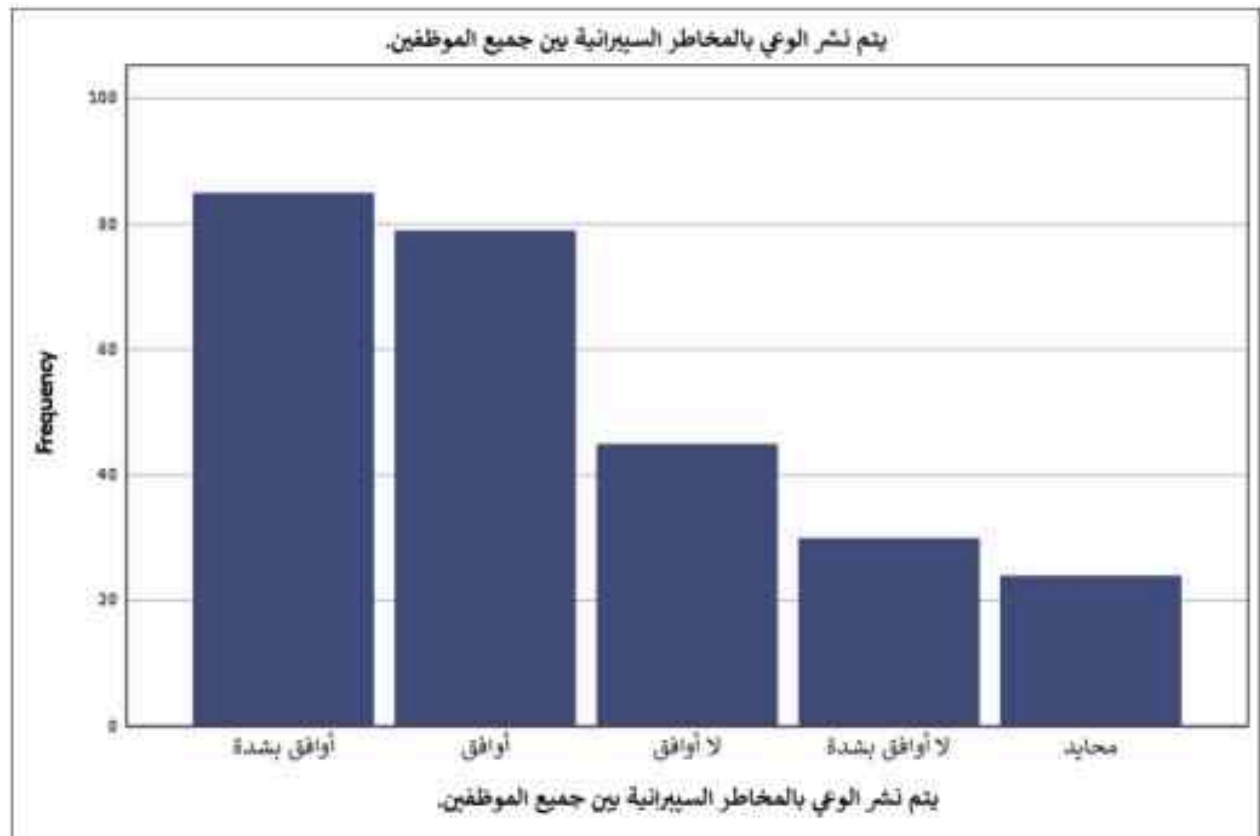
شكل توضيحي 16: التمثيل البياني لتوفر الجهة برامج تدريبية منتظمة في مجال الأمن السيبراني للعاملين.

• يتم نشر الوعي بالمخاطر السيبرانية بين جميع الموظفين.

يسجل نشر الوعي متوسطاً حسابياً مرتفعاً قدره ثلاثة فاصلة خمسة وخمسين؛ وهو من أعلى المتوسطات في الدراسة؛ مما يبرز نجاحاً كبيراً في الجانب الإعلامي والاتصالي داخل الجهة؛ فالموافقون والموافقون بشدة يمثلون اثنين وستين فاصلة أربعة بالمئة من العينة؛ وهذا التوجه يتماشى مع الحملات الوطنية للأمن السيبراني في المملكة؛ فالموظف أصبح يواجه رسائل توعوية بشكل مستمر عبر البريد أو الشاشات أو الملصقات؛ وربما يفسر الانحراف المعياري البالغ واحد فاصلة ثلاثمائة وتسعة وثمانين وجود فئات لا تصلها هذه الرسائل بفعالية؛ أو ربما يرى البعض أن التوعية سطحية ولا تتناول المخاطر الحقيقية؛ فخير "لا أوافق" و"لا أوافق بشدة" نال ثمانية وعشرين فاصلة خمسة بالمئة؛ وهي نسبة تشير إلى حاجة لتنوع أساليب الخطاب التوعوي ليصل لكافة الثقافات الوظيفية؛ فالمحايدون بنسبة تسعة فاصلة واحد بالمئة يمثلون فرصة للنحسين من خلال تبني أساليب "التلعيب" في التوعية؛ فالنتائج تؤكد أن الوعي هو المكون الأساسي لبيئة العمل الآمنة؛ فالمعرفة بالخطر هي نصف النجاة منه؛ والقيمة المرتفعة للمتوسط تعكس استثماراً ناجحاً في القوى الناعمة للأمن السيبراني؛ فصناعة الوعي تتطلب استمرارية وإبداعاً لضمان عدم ملل المتلقي؛ وهذه القراءة الإحصائية تعزز التوجه نحو قياس أثر التوعية بشكل دوري وليس مجرد عد الحملات المنفذة؛ فالموظفون يشعرون بوجود جهد توعوي مكثف؛ وهذا يقلل من احتمالات نجاح الهجمات التي تستهدف العنصر البشري؛ فالمجتمع الوظيفي الواعي يمثل سداً منيعاً يصعب اختراقه بالوسائل التقليدية؛ والنتائج تدعم التوسع في برامج "سفراء الأمن السيبراني" داخل الإدارات لتعزيز هذا الوعي ونقله للأقران بشكل عفوي ومؤثر.

جدول 28: التوزيع الإحصائي لـ نشر الوعي بالمخاطر السيبرانية بين جميع الموظفين

يتم نشر الوعي بالمخاطر السيبرانية بين جميع الموظفين.					
	Frequency	Percent	Valid Percent	Cumulative Percent	
أوافق بشدة	٨٥	٣٢,٣	٣٢,٣	٣٢,٣	Valid
أوافق	٧٩	٣٠,٠	٣٠,٠	٦٢,٤	
لا أوافق	٤٥	١٧,١	١٧,١	٧٩,٥	
لا أوافق بشدة	٣٠	١١,٤	١١,٤	٩٠,٩	
محايد	٢٤	٩,١	٩,١	١٠٠,٠	
Total	٢٦٣	١٠٠,٠	١٠٠,٠		



شكل توضيحي 17 - التمثيل البياني لنشر الوعي بالمخاطر السيبرانية بين جميع الموظفين.

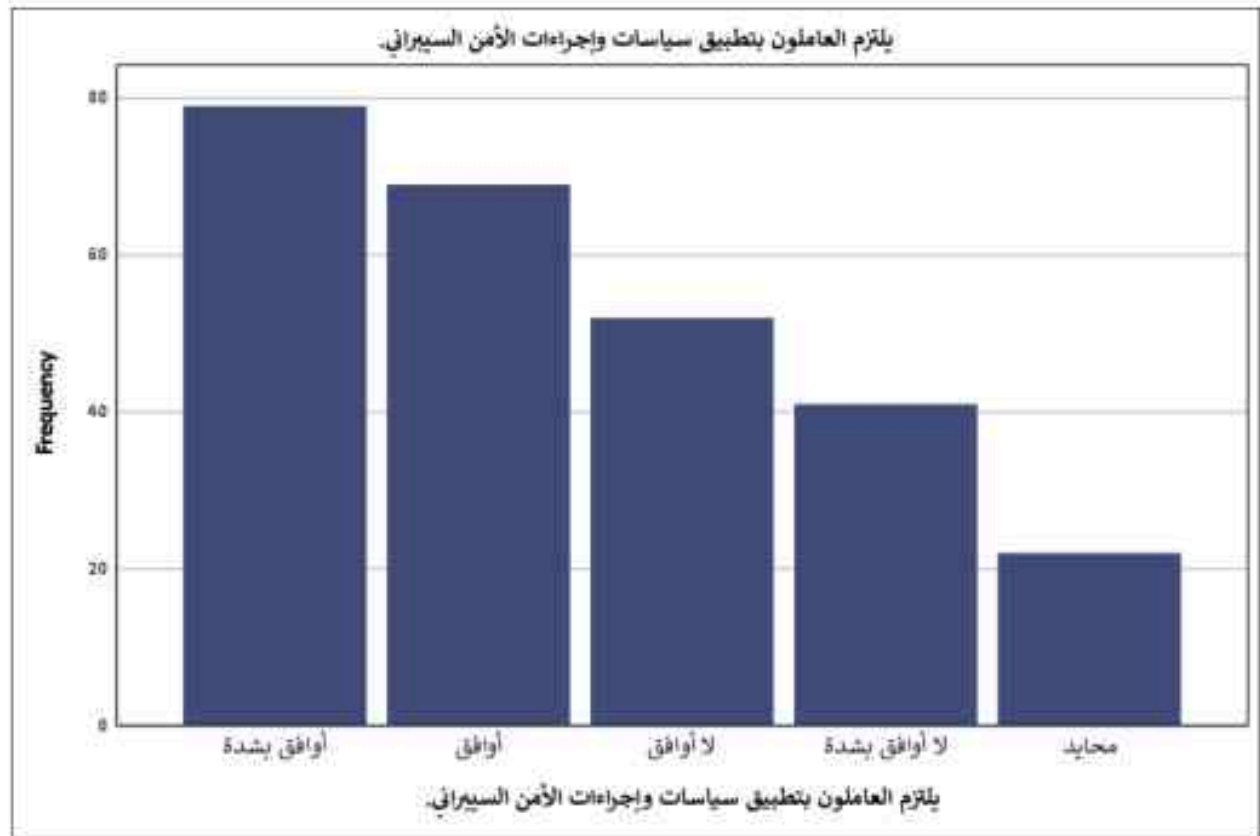
• يلتزم العاملون بتطبيق سياسات وإجراءات الأمن السيبراني.

يظهر الالتزام السلوكي متوسطاً حسابياً قدره ثلاثة فاصلة خمسة وثلاثين؛ وهو رقم يعكس تحدياً حقيقياً في تحويل الوعي إلى ممارسة؛ فخيار "أوافق بشدة" حصده ثلاثين بالمئة؛ بينما "أوافق" حصده ستة وعشرين فاصلة اثنين بالمئة؛ فالكثلة الإيجابية بلغت ستة وخمسين فاصلة اثنين بالمئة؛ وهي نسبة جيدة لكنها أقل من مستويات الوعي والتدريب المسجلة سابقاً؛ فالفجوة بين "المعرفة" و"التطبيق" تظهر بوضوح هنا؛ وربما يرجع الانحراف المعياري البالغ واحد فاصلة أربع مئة وثلاثة وسبعين إلى وجود تساهل في تطبيق العقوبات أو ضعف في الرقابة المسلكية في بعض الإدارات؛ فالموظف قد يلتزم في حضور الرقيب ويتساهل في غيابه؛ والبيانات تظهر أن خمسة وثلاثين فاصلة أربعة بالمئة لا يوافقون على وجود التزام كاف؛ وهي نسبة مرتفعة تثير القلق حول فعالية السياسات؛ فلعل بعض الإجراءات الأمنية تنسم بالتعقيد الذي يدفع الموظف للالتفاف عليها لإنجاز عمله؛ فالموازنة بين الأمان والسهولة هي مفتاح الالتزام؛ فالمحايدون بنسبة ثمانية فاصلة أربعة بالمئة قد يكونون من الفئات التي لا تحثك سياسات أمنية صارمة في عملها؛ والنتائج تستدعي تبسيط الإجراءات الأمنية ودمجها في صلب العمل اليومي بحيث يصبح

الالتزام تلقائياً؛ فالسلوك البشري هو المتغير الأصعب في معادلة الأمن؛ والقيمة المتوسطة تلمح لضرورة وجود آليات تحفيزية للالتزام بجانب الآليات الرقابية؛ فبناء ثقافة الامتثال يتطلب وقتاً وجهداً تربوياً طويلاً؛ وهذه القراءات الإحصائية تدفع نحو تبني معايير واضحة لتقييم الأداء الأمني للموظفين وربطه بالجوائز الوظيفية لضمان أعلى مستويات الانضباط الرقمي.

جدول 19: التحليل الإحصائي لالتزام العاملون بتطبيق سياسات وإجراءات الأمن السيبراني.

يلتزم العاملون بتطبيق سياسات وإجراءات الأمن السيبراني.					
	Frequency	Percent	Valid Percent	Cumulative Percent	
أوافق بشدة	٧٩	٣٠,٠	٣٠,٠	٣٠,٠	Valid
أوافق	٦٩	٢٦,٢	٢٦,٢	٥٦,٣	
لا أوافق	٥٢	١٩,٨	١٩,٨	٧٦,٠	
لا أوافق بشدة	٤١	١٥,٦	١٥,٦	٩١,٦	
محايد	٢٢	٨,٤	٨,٤	١٠٠,٠	
Total	٢٦٣	١٠٠,٠	١٠٠,٠		



شكل توضيحي 18: التمثيل البياني لالتزام العاملون بتطبيق سياسات وإجراءات الأمن السيبراني.

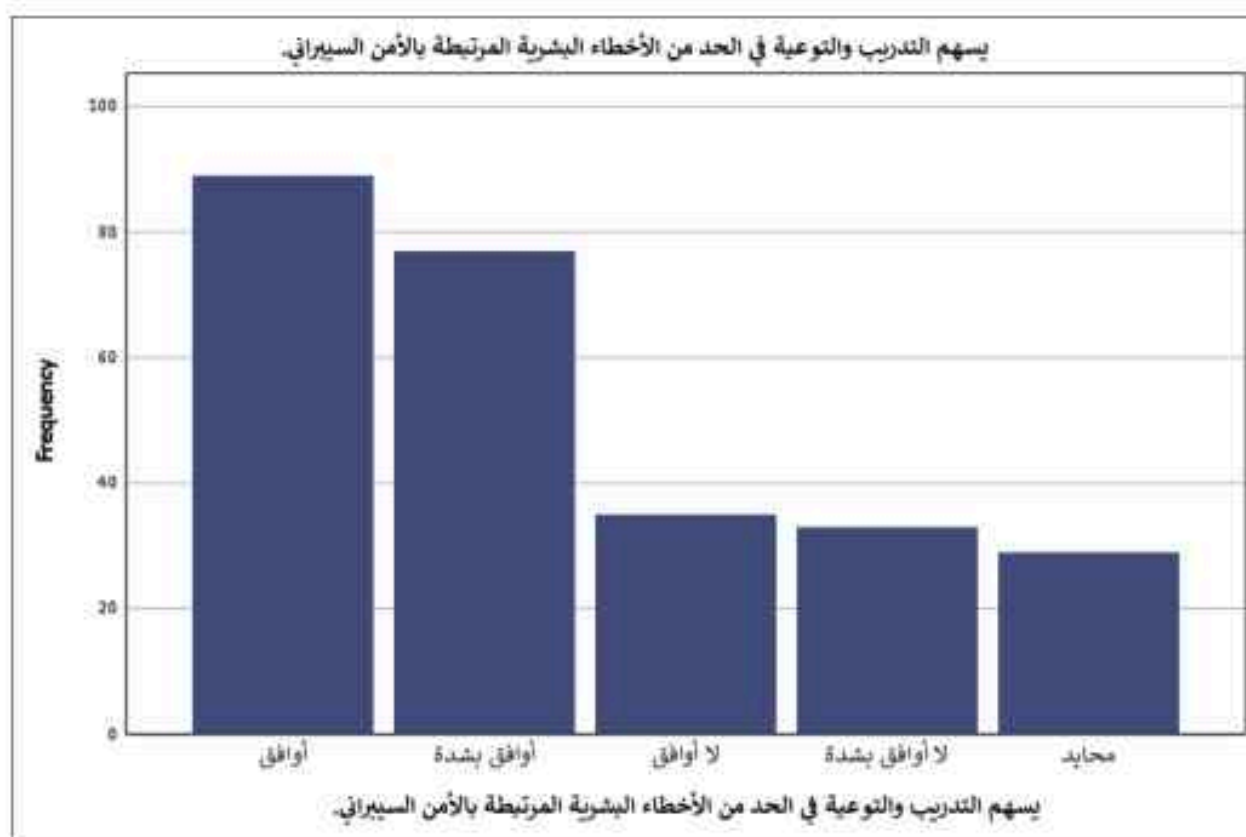
• يسهم التدريب والتوعية في الحد من الأخطاء البشرية المرتبطة بالأمن السيبراني.

تحقق هذه الفقرة متوسطاً قدره ثلاثة فاصلة أربعة وخمسين؛ مع انحراف معياري قدره واحد فاصلة ثلاثمائة وأربعة وستين؛ مما يؤكد القناعة بجدوى الاستثمار البشري؛ فالموافقون والموافقون بشدة يشكلون ثلاثة وستين فاصلة واحد بالمئة من العينة؛ وهذا الرقم يبرهن على أن الموظفين يلمسون أثر التعلم في سلوكهم التقني؛ فالتدريب يقلل من العقوبة الخطرة والجهل المسبب للثغرات؛ وربما يرجع عدم موافقة خمسة وعشرين فاصلة ثمانية بالمئة إلى رؤيتهم بأن الخطأ البشري لا يمكن تفاديه تماماً بالتدريب وحده؛ فالهندسة الاجتماعية تعتمد على نقاط ضعف نفسية قد لا يعطيها التدريب التقني الصبر؛ فالتشتت في الآراء يوجب أن هناك حاجة لتطوير المحتوى التدريبي ليركز على الجوانب السلوكية والنفسية للموظف؛ فالمحايدون بنسبة أحد عشر بالمئة قد يكونون ممن لم يختبروا أثر التدريب في مواقف حقيقية؛ فالنتائج تعزز فرضية أن الإنسان هو خط الدفاع الأول؛ والارتقاء بهذا المتوسط يتطلب بناء منظومة تدريبية تفاعلية تحاكي الهجمات الواقعية لاختبار ردود فعل الموظفين؛ فالثقة الإحصائية في أثر التدريب تمنح الإدارة مبرراً لزيادة الاستثمارات في هذا الجانب؛ فتقليل الأخطاء البشرية يعني تقليل نسبة كبيرة من الحوادث السيبرانية الناجمة؛ وهذه القراءة تدعو لربط مخرجات التدريب بنتائج التدقيق الأمني الفعلي؛ فالموظف الذي

يتدرب جيداً يجب أن تظهر نتائج تميزه في التقارير الأمنية؛ والرضا العام المسجل يبرهن على أن الجهود التوعوية تسير في الاتجاه الصحيح؛ فبناء مجتمع وظيفي مقاوم للاختراق يبدأ من تنوير العقول وتصحيح المفاهيم الخاطئة حول التعامل مع التكنولوجيا.

جدول 20 : التحليل الإحصائي لمساهمة التدريب والتوعية في الحد من الأخطاء البشرية المرتبطة بالأمن السيبراني.

يسهم التدريب والتوعية في الحد من الأخطاء البشرية المرتبطة بالأمن السيبراني.					
	Frequency	Percent	Valid Percent	Cumulative Percent	
أوافق	٨٩	٣٣,٨	٣٣,٨	٣٣,٨	Valid
أوافق بشدة	٧٧	٢٩,٣	٢٩,٣	٦٣,١	
لا أوافق	٣٥	١٣,٣	١٣,٣	٧٦,٤	
لا أوافق بشدة	٣٣	١٢,٥	١٢,٥	٨٩,٠	
محايد	٢٩	١١,٠	١١,٠	١٠٠,٠	
Total	٢٦٣	١٠٠,٠	١٠٠,٠		



شكل توضيحي 19 : التمثيل البياني لمساهمة التدريب والتوعية في الحد من الأخطاء البشرية المرتبطة بالأمن السيبراني.

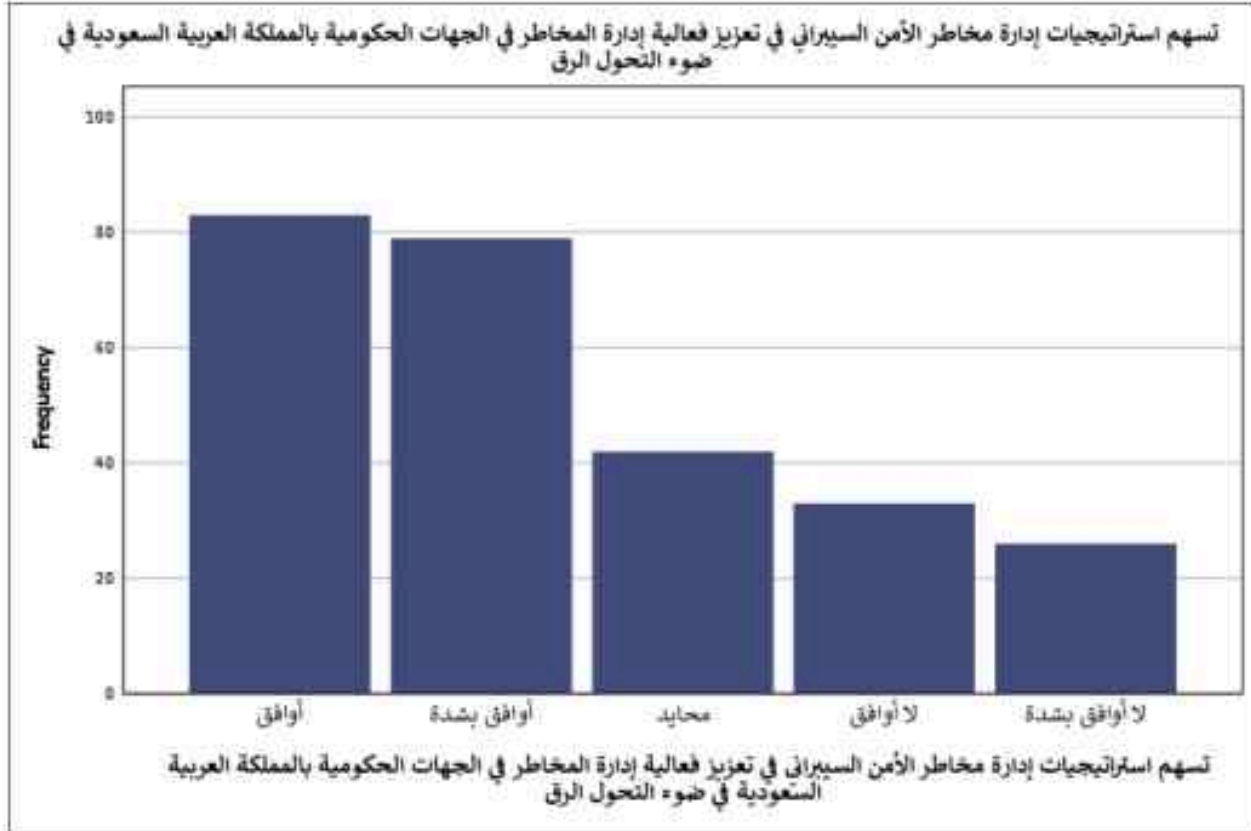
- تسهم استراتيجيات إدارة مخاطر الأمن السيبراني في تعزيز فعالية إدارة المخاطر في الجهات الحكومية بالمملكة العربية السعودية في ضوء التحول الرقمي.

تتوج هذه الفقرة الشمولية المتوسطات الحسابية بأعلى قيمة بلغت ثلاثة فاصلة تسعة وخمسين؛ مع أقل انحراف معياري في الدراسة والبالغ واحد فاصلة ثلاثمئة وواحد؛ وهذا الرقم يمثل "كلمة الفصل" من وجهة نظر المشاركين؛ فالتوافق هنا هو الأقوى والتباين هو الأقل؛ فالموافقون والموافقون بشدة يمثلون واحدًا وستين فاصلة ستة بالمئة؛ بينما تبرز فئة المحايدون بنسبة ستة عشر بالمئة كأعلى نسبة حياد مسجلة؛ ولعل هذا يرجع إلى ضخامة المفهوم وشموليته التي قد تجعل البعض يتردد في الحكم القاطع؛ فالنتائج تؤكد أن الاستراتيجيات السيبرانية هي المحرك الأساسي لنجاح إدارة المخاطر الكلية في عصر التحول الرقمي؛ فربما يتم النظر للأمن السيبراني كقائد لعملية التغيير الإداري والتقني؛ والبيانات تظهر أن نسبة الرفض (لا أوافق وبشدة) هي الأدنى حيث بلغت اثنين وعشرين فاصلة أربعة بالمئة؛ وهذا الإجماع النسبي يعكس ثقة كبيرة في التوجهات الاستراتيجية للدولة؛ فالموظفون يربطون بين أمن المعلومات وبين نجاح الرؤية الوطنية؛ فإدارة المخاطر لم تعد ترفاً إدارياً بل ضرورة وجودية للمؤسسات الرقمية؛ والقيمة المرتفعة للمتوسط تمنح صك النجاح للاستراتيجيات القائمة؛ فالمجتمع الوظيفي يدرك أن التحول الرقمي بدون أمن هو مغامرة غير محسوبة العواقب؛ وهذه القراءة الختامية تدعو لتعميق تكامل السياسات الأمنية مع أهداف العمل المؤسسي؛ فالفاعلية تكمن في التناغم بين الحماية والإنجاز؛ والارتباط الوثيق الملحوظ في الأرقام يبرهن على نضج فكري لدى الكوادر الحكومية السعودية؛ فالمستقبل الرقمي الأمن هو الهدف المشترك الذي تلتقي عنده كافة الجهود التقنية والإدارية والتدريبية التي استعرضتها الدراسة.

جدول 21: التعليل الإحصائي لمساهمة استراتيجيات إدارة مخاطر الأمن السيبراني في تعزيز فعالية إدارة المخاطر في الجهات الحكومية بالمملكة العربية السعودية في ضوء التحول الرقمي.

تسهم استراتيجيات إدارة مخاطر الأمن السيبراني في تعزيز فعالية إدارة المخاطر في الجهات الحكومية بالمملكة العربية السعودية في ضوء التحول الرقمي					
	Frequency	Percent	Valid Percent	Cumulative Percent	
Valid	أوافق	٨٣	٣١,٦	٣١,٦	
	أوافق بشدة	٧٩	٣٠,٠	٦١,٦	
	محايد	٤٢	١٦,٠	٧٧,٦	

٩٠,١	١٢,٥	١٢,٥	٣٣	لا أوافق
١٠٠,٠	٩,٩	٩,٩	٢٦	لا أوافق بشدة
	١٠٠,٠	١٠٠,٠	٢٦٣	Total



شكل توضيحي 20 - التمثيل البياني لمساهمة استراتيجيات إدارة مخاطر الأمن السيبراني في تعزيز فعالية إدارة المخاطر في الجهات الحكومية بالمملكة العربية السعودية في ضوء التحول الرقمي.

• اختبار المصادقية والموثوقية

تظهر نتائج اختبار الثبات (ألفا كرونباخ) قيمة استثنائية بلغت تسعمئة وواحد وثلاثين فاصلة صفر؛ وهي قيمة مرتفعة جداً تتجاوز بمراحل الحد الأدنى المقبول في البحوث الاجتماعية والتقنية؛ فالتجانس بين فقرات الاستبانة العشرين يعكس دقة عالية في بناء أداة الدراسة؛ وهذا الثبات المرتفع يمنح الباحث طمأنينة إحصائية بأن الأداة قادرة على تقديم نتائج مستقرة ومتسقة؛ فلو أعيد تطبيق هذه الدراسة على نفس المجتمع في ظروف مشابهة فمن المحتمل جداً الحصول على نتائج متطابقة؛ وربما يرجع هذا التفوق في الثبات إلى الوضوح اللغوي للفقرات وتغطيتها الشاملة لكافة جوانب إدارة مخاطر الأمن السيبراني؛ فالبيانات تؤكد خلو الاستجابات من العشوائية أو التناقض الصارخ؛ فالمستجيبون كانوا متسقين في آرائهم عبر كافة المحاور والارتباط

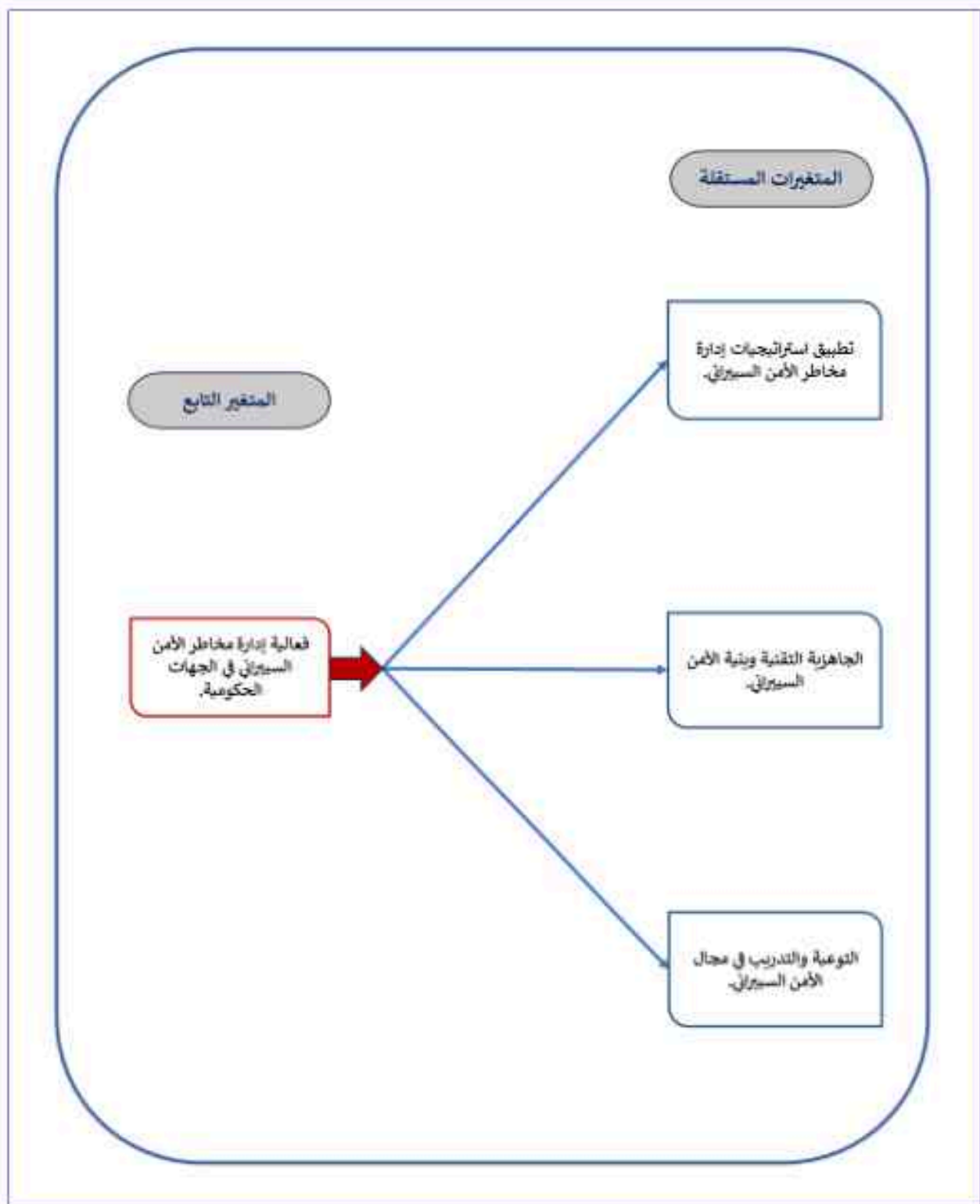
القوي بين المتغيرات يعزز من مصداقية التحليلات اللاحقة؛ فالثبات العالي هو شهادة جودة للبيانات المجمعة؛ ولعل هذا الارتفاع يعكس أيضاً وعي المستجيبين وتخصصهم؛ فالموظف الذي يمتلك درجة علمية عالية يميل للإجابة بدقة وموضوعية؛ فالقيمة المسجلة تمنح الدراسة وزناً علمياً كبيراً في الأوساط الأكاديمية؛ فالثقة في النتائج تبدأ من الثقة في الأداة؛ وهذه القراءة الإحصائية تجعل من التوصيات المبنية على الدراسة توصيات رصينة وقابلة للتطبيق العملي؛ فالمصداقية هي حجر الزاوية في أي بحث يسعى لتطوير السياسات الأمنية الوطنية؛ والنجاح في اختبار الثبات يمهد الطريق لتعميم النتائج على نطاق أوسع داخل القطاع الحكومي السعودي بكل ثقة واقتدار.

جدول 22: ملخص التحليلات الإحصائية

Case Processing Summary			
%	N		
100.0	263	Valid	Cases
.	0	Excluded ^a	
100.0	263	Total	
a. Listwise deletion based on all variables in the procedure.			

جدول 23: اختبار الثبات والموثوقية

Reliability Statistics	
N of Items	Cronbach's Alpha
20	.931



شكل توضيحي ٢١: متغيرات الدراسة التابعة والمستقلة

• تحليل الجداول المتقاطعة لمتغيرات الدراسة:

١. اختبار كاي اسكوير للعلاقة بين فعالية إدارة مخاطر الأمن السيبراني في الجهات الحكومية. وتطبيق استراتيجيات

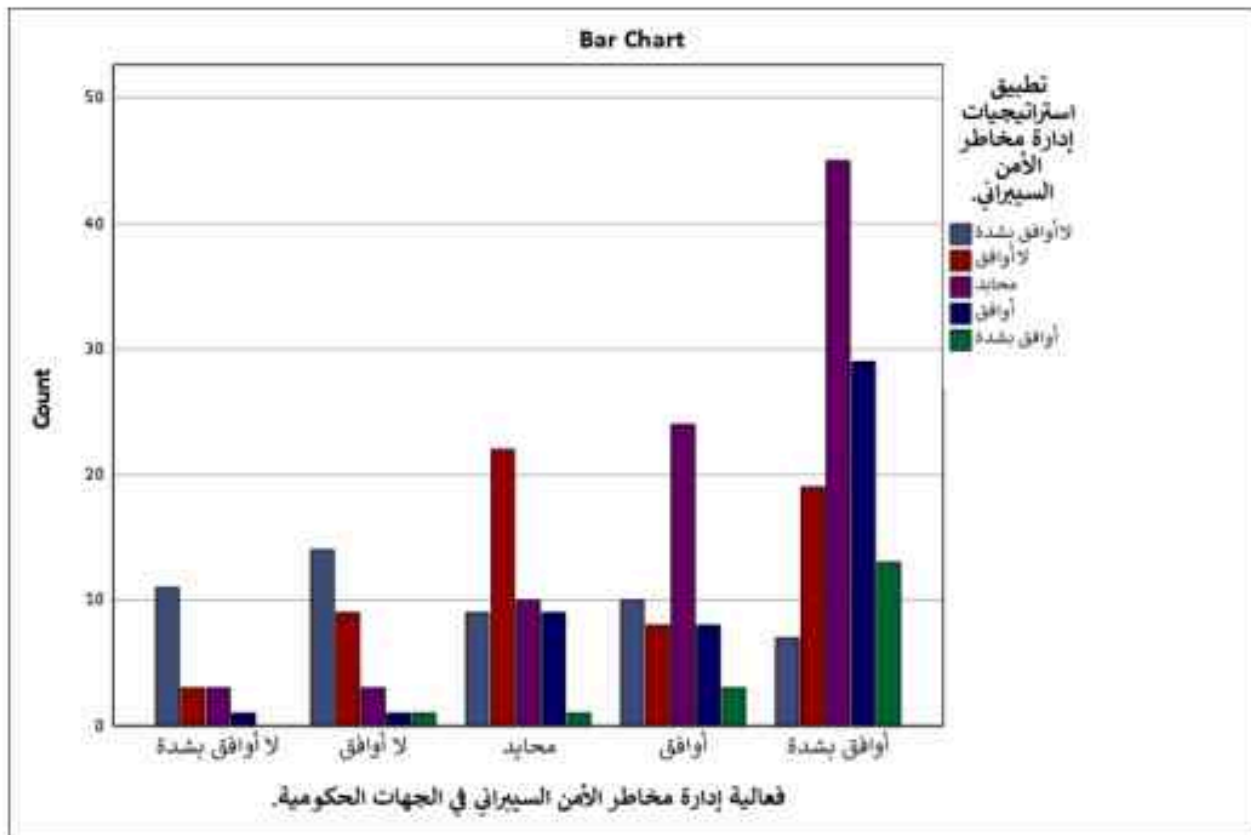
إدارة مخاطر الأمن السيبراني.

تكشف نتائج اختبار كاي اسكوير عن وجود علاقة ذات دلالة إحصائية قوية جداً عند مستوى معنوية صفر فاصلة صفرين؛ حيث بلغت قيمة الاختبار واحداً وثمانين فاصلة ثمانمئة وسبعة وستين؛ وهذا الرقم يؤكد أن النجاح في تأمين الجهة ليس مصادفة بل هو نتاج مباشر لتطبيق الاستراتيجيات الواضحة؛ فالارتباط بين التخطيط والفعالية هو ارتباط عضوي لا يمكن فصله؛ وربما يشير وجود ثمانية وعشرين بالمئة من الخلايا بقيم متوقعة أقل من خمسة إلى ضرورة الحذر في تعميم بعض التفاصيل الدقيقة؛ إلا أن القيمة الكلية تظل حاسمة في دلالتها؛ فالبيانات تبرهن على أن المؤسسات التي تتبنى استراتيجيات معلنة ومحدثة تكون أكثر قدرة على إدارة مخاطرها بكفاءة؛ فالفعل الاستراتيجي يوجه الموارد نحو التهديدات الحقيقية ويقلل من هدر الجهود في مسارات فرعية؛ ولعل هذه النتيجة تدعم التوجه نحو إلزام كافة القطاعات الحكومية بمعايير استراتيجية موحدة؛ فالدلالة الإحصائية العالية تلغي احتمالية أن يكون النجاح الأمني نتاج عوامل خارجية فقط؛ فالاستراتيجية هي المحرك الداخلي للتطوير؛ وهذه القراءة تحتل أن تحسين جودة الاستراتيجيات سيؤدي بالضرورة لرفع مستوى الفعالية الأمنية؛ فالارتباط الطردي واضح وجلي في مخرجات الجداول المتقاطعة؛ والنتائج تدعو لتعميق الفكر الاستراتيجي لدى القيادات الأمنية؛ فالتدابير التقنية بدون غطاء استراتيجي تظل منقوصة الأثر؛ فالأرقام هنا تتحدث بلغة اليقين الإحصائي عن حتمية التخطيط لضمان الأمان الرقمي؛ والبيئة السعودية بخصوصيتها الرقمية المتسارعة تجعل من هذا الارتباط شرطاً أساسياً لاستكمال مسيرة التحول الرقمي بنجاح وأمان.

جدول 2: اختبار كاي اسكوير للعلاقة بين فعالية إدارة مخاطر الأمن السيبراني في الجهات الحكومية. وتطبيق استراتيجيات إدارة مخاطر الأمن السيبراني.

Chi-Square Tests			
Asymptotic Significance (2-sided)	df	Value	
.000	16	81,867 ^a	Pearson Chi-Square
.000	16	79,082	Likelihood Ratio
.000	1	52,682	Linear-by-Linear Association
		263	N of Valid Cases

a. 7 cells (28.0%) have expected count less than 5. The minimum expected count is 1.22.



شكل توضيحي 22 : المقاييس المتمثلة للتحليل الجداول المقاطعة للعلاقة بين فعالية إدارة مخاطر الأمن السيرياني في الجهات الحكومية. وتطبيق استراتيجيات إدارة مخاطر الأمن السيرياني.

٢. اختبار كاي اسكورب للعلاقة بين فعالية إدارة مخاطر الأمن السيرياني في الجهات الحكومية. والجاهزية التقنية

وبنية الأمن السيرياني.

يسجل هذا الاختبار أعلى قيمة في دلالات الارتباط بواقع ثلاثة وتسعين فاصلة سبعمئة وعشرة؛ وبمستوى معنوية صفر فاصلة صفرين؛ مما يقطع الشك باليقين حول الدور المحوري للبنية التحتية في تحقيق الفعالية الأمنية؛ فالجاهزية التقنية ليست مجرد مكمل بل هي العمود الفقري الذي يحمل كامل منظومة إدارة المخاطر؛ فبدون أدوات رصد وحماية متطورة تظل الاستراتيجيات مجرد أخبار على ورق؛ وربما يفسر هذا الارتباط القوي سبب تركيز الجهات الحكومية على عقود التوريد التقني الكبرى؛ فالتكنولوجيا هي اللغة التي يفهمها الفضاء السيرياني؛ والبيانات تؤكد أن جودة الاستجابة للحوادث وحماية الأصول ترتبط طردياً بمدى تطور الأجهزة والبرمجيات المستخدمة؛ فلعل هذا يدفع بضرورة تحديث البنى التحتية كأولوية قصوى؛ فالجودة التقنية هي ثغرة أمنية بحد ذاتها؛ والقراءة الإحصائية تلمح إلى أن الاستثمار في البنية التحتية يعطي عائداً أمنياً مباشراً

وملموساً؛ فالارتباط العالي يقلل من احتمالات الفشل عند توفر التجهيزات المناسبة؛ وهذه النتيجة تعزز من أهمية الجولات التفتيشية التقنية للتأكد من جاهزية الأنظمة في كافة الأوقات؛ فالأرقام هنا تمنح مبرراً علمياً للميزانيات الضخمة الموجهة للأمن السيبراني؛ فالفاعلية مرتبطة بالقدرة؛ والقدرة منوطة بالجاهزية؛ والنتائج تدعم فكرة أن الأمن السيبراني هو صراع تكنولوجي في مقامه الأول يتطلب أفضل العتاد المتاح؛ والميل الإحصائي نحو هذه العلاقة يعطي رسالة واضحة لصناع القرار بأن إهمال الجانب التقني سيؤدي حتماً لانهيار المنظومة الأمنية مهما بلغت كفاءة الكوادر البشرية.

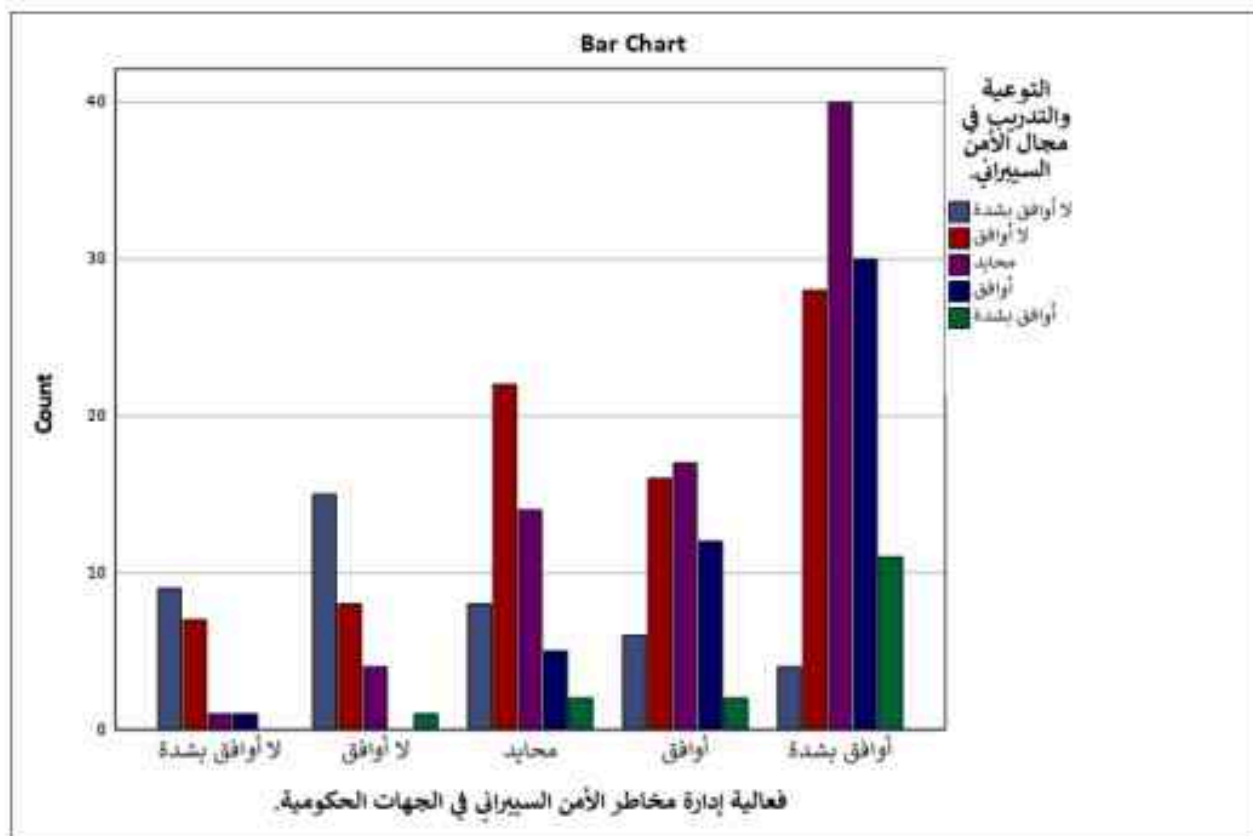
جدول 25: المخطط كافي لسكرير للعلاقة بين فعالية إدارة مخاطر الأمن السيبراني في الجهات الحكومية، والجاهزية التقنية وبلية الأمن السيبراني.

Chi-Square Tests			
Asymptotic Significance (2-sided)	df	Value	
.000	16	93,710 ^a	Pearson Chi-Square
.000	16	92,229	Likelihood Ratio
.000	1	62,383	Linear-by-Linear Association
		263	N of Valid Cases
a. 9 cells (28,0%) have expected count less than 5. The minimum expected count is .82.			

والبيئة الوظيفية التي تهتم بتنقيف أفرادها تكون أكثر مرونة في مواجهة التهديدات المتجددة: فالنوعية هي السلاح الذي لا يكلف كثيراً لكن أثره في الفعالية يضاهي الأنظمة التقنية المعقدة؛ والنتائج في مجملها تؤكد تكامل العناصر الثلاثة: الاستراتيجية، والتقنية، والبشر.

جدول 26: اختبار كاي اسكوير للعلاقة بين فعالية ادارة مختبر الأمن السيبراني في الهيئات الحكومية، والنوعية والتدريب في محك الأمن السيبراني.

Chi-Square Tests			
Asymptotic Significance (2-sided)	df	Value	
.000	16	79,352 ^a	Pearson Chi-Square
.000	16	78,541	Likelihood Ratio
.000	1	55,081	Linear-by-Linear Association
		263	N of Valid Cases
a. 7 cells (28,0%) have expected count less than 5. The minimum expected count is 1,10.			



شكل توضيحي 24: المقاييس المتماثلة لتحليل العنصر المتقطعة للعلاقة بين فعالية إدارة مخاطر الأمن السيبراني في الجهات الحكومية والتوعية والتدريب في مجال الأمن السيبراني.

• اختبار الانحدار المتعدد لمتغيرات الدراسة

يقدم نموذج الانحدار المتعدد صورة تحليلية عميقة للأثر التراكمي للمتغيرات المستقلة على الفعالية الأمنية: فقد بلغت قيمة معامل الارتباط (R) ستمئة وسبعة وثلاثين فاصلة صفر؛ بينما سجل معامل التحديد (R Square) أربعمئة وخمسة فاصلة صفر؛ مما يعني أن المتغيرات الثلاثة (الاستراتيجيات، الجاهزية، التدريب) تفسر مجتمعة أربعين فاصلة خمسة بالمئة من التباين الحاصل في فعالية إدارة مخاطر الأمن السيبراني؛ وهذه النسبة تعتبر جيدة جداً في العلوم الإدارية والتقنية نظراً لوجود عوامل أخرى خارجية قد لا تشملها الدراسة؛ وربما يبرز معامل ($Beta$) أن الجاهزية التقنية هي المؤثر الأكبر بقيمة ثلاثمئة واثنين وعشرين فاصلة صفر؛ تلها الاستراتيجيات بقيمة مئتين وتسعين فاصلة صفر؛ ثم التدريب بمائتين وثمانية وخمسين فاصلة صفر؛ فكل المتغيرات تمتلك دلالة إحصائية عند مستوى صفر فاصلة صفرين؛ مما يؤكد أن تحسين أي منها سيؤدي بالضرورة لرفع الفعالية؛ فالبيانات تظهر أن النموذج ككل يمتلك قدرة تنبؤية عالية تؤكدتها قيمة (F) البالغة ثمانية وخمسين فاصلة ثمانمئة وواحد وثلاثين؛ فالعلاقة الخطية بين هذه العوامل والنجاح الأمني علاقة حقيقية وليست وليدة الصدفة؛ فلعل هذا يدفع نحو ضرورة التطوير المتوازي لكافة المسارات؛ فإهمال التدريب مثلاً سيخفض الفعالية الكلية حتى لو كانت التقنيات

متطورة: والنماذج تعطي خريطة طريق واضحة للمسؤولين حول مواضيع الاستثمار الأنجع: فالمعادلة الإحصائية تضع وزناً نسبياً لكل عنصر؛ وهذا التحليل الاتحادي يمنح الدراسة قدرة على استشراف المستقبل الأمني بناءً على المعطيات الحالية؛ فالفاعلية هي محصلة لجهود متكاملة وليست نتاج عامل واحد منفصل.

جدول 27: ملخص النموذج

Model Summary ^b				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.637 ^a	.405	.398	.993
a. Predictors: (Constant), التنوع والتدريب في مجال الأمن السيبراني، تطبيق استراتيجيات إدارة مخاطر الأمن السيبراني، الجاهزية التقنية وبناءة الأمن السيبراني.				
b. Dependent Variable: فاعلية إدارة مخاطر الأمن السيبراني في الجهات الحكومية.				

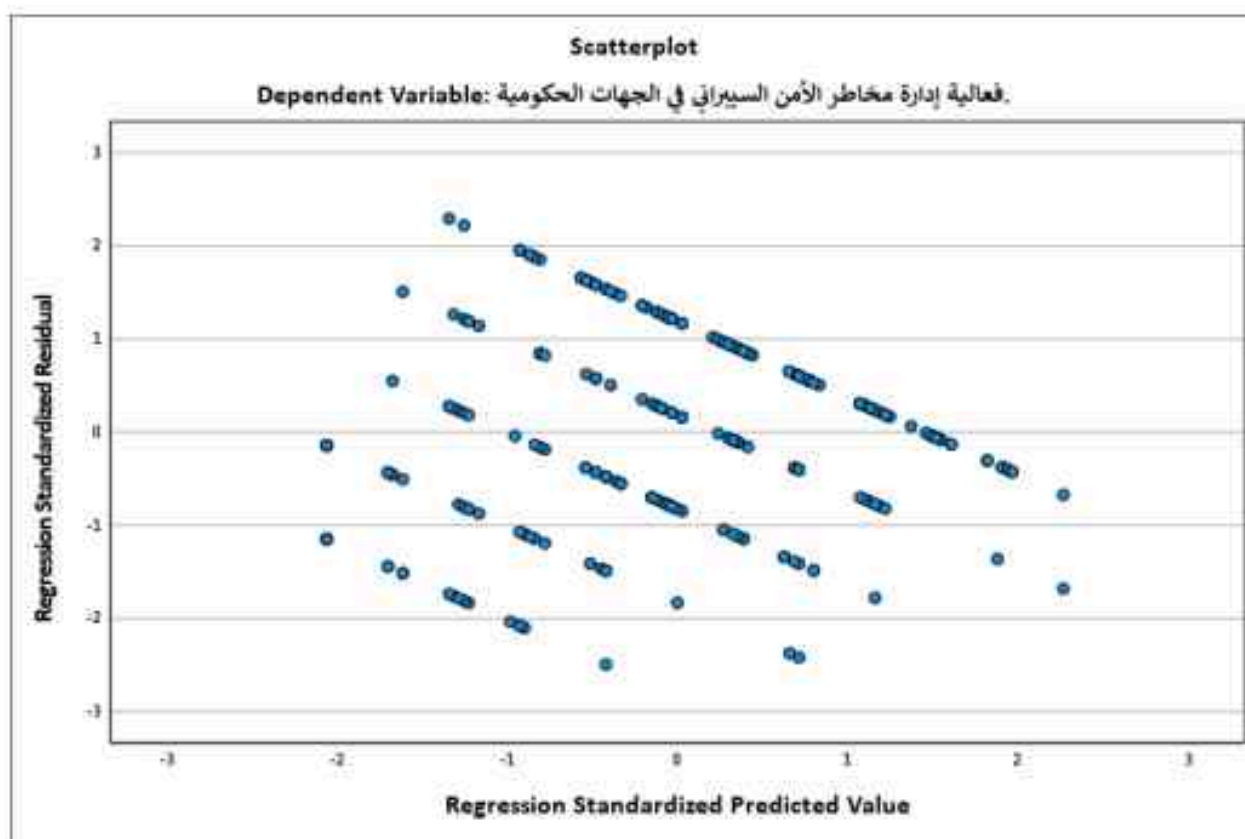
جدول 28: تحليل التباين

ANOVA ^a					
Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	173,959	3	57,986	58,831	.000 ^b
Residual	255,281	259	.986		
Total	429,240	262			
a. Dependent Variable: فاعلية إدارة مخاطر الأمن السيبراني في الجهات الحكومية.					
b. Predictors: (Constant), التنوع والتدريب في مجال الأمن السيبراني، تطبيق استراتيجيات إدارة مخاطر الأمن السيبراني، الجاهزية التقنية وبناءة الأمن السيبراني.					

جدول 29: معاملات تحليل الانحدار المتعدد

Coefficients ^a						
Sig.	t	Standardized Coefficients	Unstandardized Coefficients		Model	
		Beta	Std. Error	B		
.000	5,575		.209	1,165	(Constant)	1

٠.٠٠٠	٥,٦٩٠	٠.٢٩٠	٠.٥٥	٠.٣١٦	تطبيق استراتيجيات إدارة مخاطر الأمن السيبراني.
٠.٠٠٠	٦,١٧٩	٠.٣٢٢	٠.٥٩	٠.٣٦٤	الجاهزية التقنية وبناء الأمن السيبراني.
٠.٠٠٠	٤,٩١١	٠.٢٥٨	٠.٦٠	٠.٢٩٣	التوعية والتدريب في مجال الأمن السيبراني.
Dependent Variable: فعالية إدارة مخاطر الأمن السيبراني في الجهات الحكومية.					



شكل توطيني 25: شكل الانتشار الدولي

قطاع الامتياز الامن السيبراني في الجهات الحكومية				
خلق استراتيجيات مخاطر الامن السيبراني				
العملية التقنية وبناء الامن السيبراني				
التوعية والتدريب في مجال الامن السيبراني				
	فعالية إدارة مخاطر الامن السيبراني في الجهات الحكومية	تطبيق استراتيجيات إدارة مخاطر الامن السيبراني	الجاهزية التقنية وبناء الامن السيبراني	التوعية والتدريب في مجال الامن السيبراني

شكل توضيحي 26 : مصفوفة شكل الانتشار

● اختبار التباين الأحادي للمتغيرات الدراسة

تؤكد نتائج تحليل التباين (ANOVA) معنوية النموذج الاحتمالي للدراسة بوجود قيمة (F) تصل إلى سبعة عشر فاصلة خمسمئة وسبعة وسبعين؛ وبدلالة إحصائية قاطعة عند الصفر؛ وهذا يشير إلى وجود فروق حقيقية وجوهرية في مستويات الفعالية تعزى إلى الاختلاف في تطبيق المتغيرات المستقلة؛ فالتفاوت في الأداء الأمني بين الجهات ليس عشوائياً بل له أسباب إحصائية مفسرة؛ وربما يظهر مجموع المربعات (Sum of Squares) أن الانحدار يفسر جزءاً كبيراً من التباين الكلي؛ مما يعزز من كفاءة النموذج المستخدم؛ فالبيانات تبرهن على أن العينة بمختلف فئاتها أجمعت على أن هذه العوامل هي المحرك الفعلي للنجاح؛ فالاختبار يلقي فرضية العدم التي تدعي عدم وجود أثر لهذه المتغيرات؛ فلعل هذه النتيجة تكون حافزاً للجهات ذات الأداء المنخفض لمراجعة سياساتها في ضوء هذه المتغيرات؛ فالتباين المرصود يفتح المجال لتبادل الخبرات بين القطاعات الحكومية؛ فالنجاح الذي حققته بعض الجهات يمكن تفسيره إحصائياً من خلال تفوقها في هذه المحاور؛ والقراءات هنا تمنح الدراسة صلابة منهجية وتجعل من نتائجها مرجعاً موثقاً لصناعة القرار؛ فالعلاقة السببية بين المدخلات (الاستراتيجية، التقنية،

البشر) والمخرجات (الفعالية) باتت واضحة إحصائياً: وهذه النتائج تدعم فكرة المأسمة الشاملة للأمن السيبراني كمنظومة متكاملة لا تقبل التجزئة؛ فالنناغم بين العناصر هو ما يخلق الفارق في النتائج النهائية للحماية الرقمية.

يأتي معامل بايز (Bayes Factor) ليتوج التحليلات الإحصائية بقيمة مذهلة تتجاوز الأرقام المألوفة: مما يعطي أدلة قاطعة تدعم النموذج المقترح مقابل النموذج الصفرى؛ فالتفوق الهائل لهذا المعامل يبرهن على أن المتغيرات المستقلة المختارة تمتلك قوة تفسيرية لا تدع مجالاً للشك؛ فالعلاقة بين التدريب والجاهزية والاستراتيجيات وبين فعالية إدارة المخاطر هي حقيقة إحصائية راسخة؛ وربما يمثل معامل التحديد المعدل (Adjusted R Square) البالغ أربع عشرة وأثنين وثلاثين فاصلة صفر مؤشراً على كفاءة النموذج حتى بعد ضبط درجات الحرية؛ فالبيانات تكشف عن دقة عالية في تقدير المعالم؛ فـنموذج بايز يذهب إلى ما هو أبعد من الدلالة التقليدية ليؤكد قوة الدليل العلمي المتوفر؛ فلعل هذه القيمة الفلكية للمعامل تعكس التناسق الشديد في استجابات العينة الكبيرة (مائتان وثلاثة وستون مشاركاً)؛ فالنتائج تمنح الدراسة مصداقية عالمية تتجاوز الحدود المحلية؛ فالدليل البايزي هو المعيار الحديث في التحليل الإحصائي المتقدم؛ وهذه القراءة الختامية تلخص جوهر الدراسة في أن أمن البيئة الرقمية السعودية يستند إلى ركائز علمية مثبتة قابلة للقياس والتنبؤ؛ فالثقة في فعالية إدارة المخاطر هي ثقة مبنية على براهين رقمية صلبة؛ والنموذج يثبت نجاحه في استنطاق الواقع وتحويله إلى مؤشرات أداء دقيقة؛ فالمستقبل الرقمي للمملكة في ظل هذه النتائج يبدو محصلاً بمنهجيات إدارية وتقنية واعية ومدروسة بعناية فائقة؛ فالأرقام في النهاية تبتسم للجهود المنظمة والتخطيط الواعي.

جدول 30: اختبار التباين الأحادي

ANOVA ^{a,b}					
Sig.	F	Mean Square	df	Sum of Squares	Source
.000	17,577	16,369	12	196,424	Regression
		.931	250	232,815	Residual
			262	429,240	Total
a. Dependent Variable: فعالية إدارة مخاطر الأمن السيبراني في الجهات الحكومية.					
b. Model: (Intercept), التطبيق استراتيجيات إدارة مخاطر الأمن السيبراني.. التوعية والتدريب في مجال الأمن السيبراني.. الجاهزية التقنية وبناء الأمن السيبراني.					

جدول 32: ملخص نموذج معامل بايز

Bayes Factor Model Summary ^{a,b}				
Std. Error of the Estimate	Adjusted R Square	R Square	R	Bayes Factor ^c
.97	.432	.458	.676	3.678397381279235.....,...

a. Method: JZS

b. Model: (Intercept),
تطبيق استراتيجيات إدارة مخاطر الأمن السيبراني.. التوعية والتدريب في مجال الأمن السيبراني.. الجاهزية التقنية وبناء الأمن السيبراني.

c. Bayes factor: Testing model versus null model (Intercept).

أظهرت نتائج الدراسة أن استراتيجيات إدارة مخاطر الأمن السيبراني تؤدي دورًا محوريًا في تعزيز فعالية إدارة المخاطر داخل الجهات الحكومية بالمملكة العربية السعودية، حيث تبين وجود تأثير إيجابي ذي دلالة إحصائية للمتغيرات المستقلة المتمثلة في تطبيق استراتيجيات إدارة مخاطر الأمن السيبراني، والجاهزية التقنية وبناء الأمن السيبراني، والتوعية والتدريب في مجال الأمن السيبراني على المتغير التابع المتمثل في فعالية إدارة مخاطر الأمن السيبراني. وتعكس هذه النتائج مستوى الاهتمام المتزايد الذي توليه الجهات الحكومية السعودية لتطوير منظومات الأمن السيبراني بما يتوافق مع برامج التحول الرقمي ورؤية المملكة العربية السعودية ٢٠٣٠، والتي جعلت الأمن السيبراني أحد المرتكزات الأساسية لاستدامة الخدمات الحكومية الرقمية.

وأوضحت النتائج أن تطبيق استراتيجيات إدارة مخاطر الأمن السيبراني جاء من أكثر العوامل تأثيرًا في رفع فعالية إدارة المخاطر، وهو ما يؤكد أن وجود سياسات واضحة، وخطط استجابة للحوادث، وآليات دورية لتقييم المخاطر، يسهم بصورة مباشرة في تحسين قدرة الجهات الحكومية على التنبؤ بالمخاطر الإلكترونية والحد من أثارها. كما تشير هذه النتيجة إلى أن الإدارة الاستراتيجية للمخاطر أصبحت عنصرًا أساسيًا في نجاح المؤسسات الحكومية، خاصة مع ازدياد الاعتماد على الخدمات الرقمية والأنظمة الإلكترونية، الأمر الذي يتطلب دمج إدارة المخاطر ضمن عمليات التخطيط الاستراتيجي واتخاذ القرار.

كما بينت النتائج أن الجاهزية التقنية وبناء الأمن السيبراني تمثل أحد المرتكزات الأساسية لتعزيز فعالية إدارة المخاطر، حيث إن امتلاك الجهات الحكومية لبنية تحتية رقمية متطورة، وأنظمة متقدمة للحماية، وأدوات فعالة لمراقبة الشبكات واكتشاف الهجمات الإلكترونية، يسهم في رفع مستوى الجاهزية وتقليل احتمالية التعرض للاختراقات الأمنية. وتؤكد هذه النتيجة أن نجاح استراتيجيات الأمن السيبراني لا يتحقق من خلال السياسات والإجراءات فقط، وإنما يعتمد أيضًا على توافر تقنيات حديثة قادرة على مواكبة التطورات المتسارعة في طبيعة التهديدات السيبرانية.

وأظهرت النتائج كذلك أن التوعية والتدريب في مجال الأمن السيبراني كان لهما أثر إيجابي واضح في تعزيز فعالية إدارة مخاطر الأمن السيبراني، مما يعكس أهمية العنصر البشري بوصفه أحد أهم مكونات منظومة الأمن السيبراني. فارتقاء مستوى الوعي الأمني لدى العاملين يقلل من احتمالات وقوع الأخطاء البشرية التي تُعد من أبرز أسباب الحوادث السيبرانية، كما يسهم في رفع قدرة الموظفين على اكتشاف التهديدات والإبلاغ عنها والاستجابة لها وفق الإجراءات المعتمدة. وتشير هذه النتيجة إلى أن الاستثمار في تنمية الكفاءات البشرية لا يقل أهمية عن الاستثمار في التقنيات الأمنية الحديثة.

وتتفق نتائج الدراسة مع نظرية إدارة المخاطر المؤسسية (Enterprise Risk Management - ERM) ، التي تؤكد أن فعالية إدارة المخاطر تتحقق من خلال تكامل الجوانب التنظيمية والتقنية والبشرية ضمن إطار مؤسسي موحد. كما تتوافق مع العديد من الدراسات السابقة التي أشارت إلى أن المؤسسات التي تعتمد منهجًا استراتيجيًا في إدارة المخاطر السيبرانية تكون أكثر قدرة على حماية أصولها الرقمية، وضمان استمرارية الأعمال، وتعزيز الثقة في خدماتها الرقمية، ويعزز هذا التوافق من قوة النموذج النظري للدراسة، ويؤكد ملاءمته لتفسير واقع الأمن السيبراني في الجهات الحكومية السعودية.

ومن الناحية التطبيقية، تشير النتائج إلى أن الجهات الحكومية مطالبة بتبني نهج استباقي في إدارة المخاطر السيبرانية، يقوم على التحديث المستمر للاستراتيجيات الأمنية، والاستثمار في التقنيات الحديثة، وتعزيز الشراكة بين الإدارات المختلفة، بما يضمن بناء منظومة أمنية متكاملة قادرة على مواجهة التهديدات المستقبلية. كما تؤكد النتائج أن الأمن السيبراني أصبح عنصرًا أساسيًا في نجاح التحول الرقمي، وأن تحقيق أهداف الحكومة الرقمية يتطلب وجود بيئة رقمية آمنة ومرنة تحافظ على سرية البيانات وسلامتها واستمرارية الخدمات الحكومية.

الخاتمة

خلصت الدراسة إلى أن فعالية استراتيجيات إدارة مخاطر الأمن السيبراني تمثل أحد العوامل الجوهرية لضمان نجاح برامج التحول الرقمي في الجهات الحكومية بالمملكة العربية السعودية. وقد أثبتت النتائج أن تطبيق استراتيجيات واضحة لإدارة المخاطر، وتوفير بنية تقنية متطورة، وتعزيز برامج التوعية والتدريب، تؤدي جميعها إلى رفع مستوى فعالية إدارة المخاطر السيبرانية، وتحسين قدرة الجهات الحكومية على مواجهة التهديدات الرقمية وحماية أصولها المعلوماتية.

كما أكدت الدراسة أن الأمن السيبراني لم يعد يقتصر على الجانب التقني، بل أصبح منظومة إدارية واستراتيجية متكاملة ترتبط بالحوكمة، وإدارة المخاطر، واستمرارية الأعمال، وصنع القرار. ولذلك فإن نجاح الجهات الحكومية في تحقيق أهداف التحول الرقمي يعتمد إلى حد كبير على قدرتها على دمج الأمن السيبراني ضمن خططها الاستراتيجية، وتطوير سياسات مرنة تستجيب للتغيرات المتسارعة في البيئة الرقمية.

وأبرزت الدراسة كذلك أهمية العنصر البشري باعتباره أحد أهم مكونات منظومة الأمن السيبراني، حيث تبين أن رفع مستوى الوعي الأمني والتدريب المستمر يساهمان في الحد من المخاطر الناتجة عن الأخطاء البشرية، وتعزيزان من قدرة المؤسسات على الاستجابة للحوادث السيبرانية بصورة أكثر كفاءة. كما أن تطوير البنية التحتية التقنية واعتماد الحلول الذكية في مراقبة الشبكات وتحليل التهديدات أصبح ضرورة لضمان استدامة الخدمات الحكومية الرقمية.

وتختتم الدراسة بالتأكيد على أن نتائجها تقدم قيمة علمية وعملية يمكن أن تستفيد منها الجهات الحكومية السعودية عند تطوير استراتيجيات إدارة مخاطر الأمن السيبراني، كما تمثل منطلقاً لإجراء دراسات مستقبلية تتناول متغيرات إضافية ترتبط بالحوكمة الرقمية، والذكاء الاصطناعي، والمرونة السيبرانية، بما يساهم في تعزيز جاهزية القطاع الحكومي لمواجهة التهديدات الرقمية وتحقيق مستهدفات رؤية المملكة العربية السعودية ٢٠٣٠.

التوصيات

استنادًا إلى النتائج التي أظهرت وجود تأثير إيجابي لتطبيق استراتيجيات إدارة مخاطر الأمن السيبراني، والجاهزية التقنية، وبرامج التوعية والتدريب في تعزيز فعالية إدارة مخاطر الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية، توصي الدراسة بما يأتي:

١. تطوير استراتيجيات شاملة ومتكاملة لإدارة مخاطر الأمن السيبراني تتوافق مع أهداف الجهات الحكومية ومتطلبات التحول الرقمي.
٢. تحديث سياسات وإجراءات الأمن السيبراني بصورة دورية لمواكبة التهديدات الإلكترونية المتجددة والتقنيات الحديثة.
٣. تعزيز الاستثمار في البنية التحتية التقنية، وتحديث أنظمة الحماية، وأدوات كشف التهديدات والاستجابة للحوادث السيبرانية.
٤. زيادة برامج التدريب والتوعية المستمرة لجميع العاملين في الجهات الحكومية، مع التركيز على الوقاية من التصيد الإلكتروني والهندسة الاجتماعية وأفضل الممارسات الأمنية.
٥. تبني أليات دورية لتقييم وإدارة المخاطر السيبرانية باستخدام معايير وأطر عالمية مثل ISO/IEC ٢٧٠٠١ أو NIST Cybersecurity Framework.
٦. إنشاء مؤشرات أداء رئيسية (KPIs) لقياس فعالية استراتيجيات إدارة مخاطر الأمن السيبراني ومتابعة تنفيذها بصورة مستمرة.
٧. تعزيز التكامل والتنسيق بين إدارات الأمن السيبراني وتقنية المعلومات وإدارة المخاطر والإدارة العليا لضمان سرعة اتخاذ القرار أثناء الحوادث السيبرانية.
٨. توسيع استخدام تقنيات الذكاء الاصطناعي والتحليلات التنبؤية في اكتشاف التهديدات السيبرانية والاستجابة الاستباقية لها.
٩. إجراء اختبارات واختراقات أمنية دورية، وتنفيذ تمارين محاكاة للاستجابة للحوادث السيبرانية لرفع مستوى الجاهزية المؤسسية.
١٠. تشجيع الباحثين على إجراء دراسات مستقبلية تتناول متغيرات إضافية مثل الحوكمة الرقمية، والثقافة التنظيمية، والذكاء الاصطناعي، ومدى تأثيرها في تعزيز فعالية إدارة مخاطر الأمن السيبراني في القطاع الحكومي.

المراجع

Abn_hammad, M. Z. (٢٠٢٥). The Evolution of E-Government in Saudi Arabia: A Comprehensive Review of Digital Transformation Strategies, Institutional Readiness, and Citizen-Centric Service Delivery in The Vision ٢٠٣٠ Era. Retrieved from

https://www.researchgate.net/publication/٣٩٤٩١٦٦٥٣/The_Evolution_of_EGovernment_in_Saudi_Arabia_A_Comprehensive_Review_of_Digital_Transformation_Strategies_Institutional_Readiness_and_CitizenCentric_Service_Delivery_in_The_Vision_٢٠٣٠_Era

Alhakami, W. (٢٠٢٤). Enhancing Cybersecurity Competency in the Kingdom of Saudi Arabia: A Fuzzy Decision-Making Approach. Retrieved from

<https://www.sciencedirect.com/org/science/article/pii/S١٥٤٦٣٢١٨٢٤-٠-٢٤٤٣>

Al-Hawamleh, A. M. (٢٠٢٤). Investigating the multifaceted dynamics of cybersecurity practices and their impact on the quality of e-government services: evidence from the KSA. Retrieved from

<https://www.emerald.com/dprg/article/٢٦/٣/٣١٧/١٢٢٣٧٥-/Investigating-themultifaceted-dynamics-of>

Alkhalifa, M. (٢٠٢٤). Top ٥ Deadly Cybersecurity Threats to Kingdom of Saudi Arabia. Retrieved from

<https://www.preprints.org/manuscript/٢٠٢٤-٨,٢٢٤٤>

Assiri, K. (٢٠٢٢). Security Challenges for Digital Transformation in Saudi Arabia. Retrieved from

https://www.researchgate.net/publication/٣٦٦٦٢٠٠٥١/Security_Challenges_for_Digital_Transformation_in_Saudi_Arabia

Bennouk, K. (٢٠٢٤). A Comprehensive Review and Assessment of Cybersecurity Vulnerability Detection Methodologies. Retrieved from <https://www.mdpi.com/٢٦٢٤-٨٠٠-X/٤/٤/٤٠>

Haque, G. M. (٢٠٢٥). Cybersecurity Risk Management in the Age of Digital Transformation: A Systematic Literature Review. Retrieved from

https://www.researchgate.net/publication/٣٩٤٥٤٩١٤٩/Cybersecurity_Risk_Management_in_the_Age_of_Digital_Transformation_A_Systematic_Literature_Review

Hossain, S. T. (٢٠٢٥). Cybersecurity in local governments: A systematic review and framework of key challenges. Retrieved from <https://www.sciencedirect.com/science/article/pii/S٢٦٦٤٣٢٨٦٢٤-٠-٧٩٢>

Jalali, p. S. (٢٠١٩). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. Retrieved from

<https://www.sciencedirect.com/science/article/pii/S٠٩٦٣٨٦٨٧١٧٣-٤٣٥٣>

Johri, A. (٢٠٢٣). Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation. Retrieved from

<https://www.semanticscholar.org/paper/Exploring-Customer-Awareness-towards-Their-Cyber-in-Johri-Kumar/271f1fe9Vabc782120f3.d0-1.0c7ecAdVaTTe1c>

Knowles, M. (2026). Cybersecurity Risk Management: Frameworks, Best Practices and Audit Readiness. Retrieved from <https://hyperproof.io/resource/cybersecurity-riskmanagement-process/>

Melaku, H. M. (2022). Context-Based and Adaptive Cybersecurity Risk Management Framework. Retrieved from <https://www.mdpi.com/2227-9911/11/7/1111>

Nygard, K. E. (2021). Dimensions of Cybersecurity Risk Management. Retrieved from https://www.researchgate.net/publication/3524330013_Dimensions_of_Cybersecurity_Risk_Management

Radebe, M. J. (2024). Public Sector Communication in the Digital Age. Retrieved from https://www.researchgate.net/publication/384904477_Public_Sector_Communication_in_the_Digital_Age

Saeed, S. (2020). Digital Transformation in Governmental Public Service Provision and Usable Security Perception in Saudi Arabia. Retrieved from <https://www.mdpi.com/2078-2489/17/3/2457>

Slapničar, S. (2020). Cyber risk management: an illusion of a risk-based approach. Retrieved from <https://link.springer.com/article/10.1007/s00187-020-00411-2>

الملاحق

الموضوع: طلب تحكيم استبيان بحثي

الدكتور/..... المحترم،

السلام عليكم ورحمة الله وبركاته،

أتمنى أن تكونوا بخير وبأفضل حال.

أود إبلاغكم بأنني طالب في جامعة ميدأوشن - كلية الإدارة - تخصص ماجستير في إدارة مخاطر، وأعمل حالياً على بحث بعنوان "فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية في ضوء التحول الرقمي"، وذلك كجزء من متطلبات درجة الماجستير في إدارة مخاطر.

أتوجه إليكم بهذا الطلب لأستفيد من خيراتكم القيمة في تحكيم الاستبيان الخاص ببحثي. أرفق لكم نسخة من الاستبيان، وأرجو منكم التكرم بمراجعتها وإبداء ملاحظاتكم واقتراحاتكم حول مدى دقة وملاءمة العبارات المطروحة لقياس الأهداف المرجوة من الدراسة كما أرجو منكم اقتراح أي تعديلات ترونها مناسبة سواء بإعادة صياغة العبارات، أو حذفها، أو إضافة عبارات جديدة. أشكركم جزيل الشكر على وقتكم وجهودكم، وأتطلع إلى تلقي ملاحظاتكم القيمة.

مع خالص التقدير والاحترام..

مشاري علي العربي

طالب ماجستير إدارة مخاطر

كلية الإدارة، جامعة ميدأوشن

الاستبيان

بسم الله الرحمن الرحيم

السيد/..... المحترم،

السلام عليكم ورحمة الله وبركاته،

أود إبلاغكم بأنني طالب في جامعة ميدأوشن - كلية الإدارة - تخصص ماجستير في إدارة مخاطر، وأعمل حالياً على بحث بعنوان "فاعلية استراتيجيات إدارة مخاطر الأمن السيبراني في الجهات الحكومية بالمملكة العربية السعودية في ضوء التحول الرقمي"، كجزء من متطلبات درجة الماجستير في إدارة مخاطر. ونظراً لأهمية آرائكم القيمة، أرجو منكم التفضل بالإجابة على هذا الاستبيان وأؤكد لكم أن إجاباتكم ستكون محل تقدير كبير وستعامل بسرية تامة، ولن تستخدم إلا لأغراض البحث العلمي. لذا أرجو أن تكون إجاباتكم دقيقة وصادقة قدر الإمكان للمساهمة في تحقيق نتائج دقيقة.

شاكر لكم حسن تعاونكم

مشاري علي العريني

طالب ماجستير إدارة مخاطر

كلية الإدارة جامعة ميدأوشن

المشرفين

أ.د. الفيصل عيد الحميد محمد

أ.د. فايز علي جراد

كلية الإدارة، جامعة ميدأوشن

الاستبانة

الاستبانة					الإجابة
١- الاستبانة العامة					
العمر	٢٠-٣٠	٣٠-٤٠	٤٠-٥٠	٥٠-٦٠	٦٠+
الجنس	ذكر	أنثى			
الدرجة العلمية	شهادة الدراسة الثانوية	درجة البكالوريوس	شهادة عليا	ماجستير	دكتوراه
٢- أسئلة الاستبيان					
تطبق الجهة الحكومية استراتيجيات واضحة لإدارة مخاطر الأمن السيبراني.	لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
يتم تحديث استراتيجيات الأمن السيبراني بشكل دوري لمواكبة التهديدات الحديثة.	لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
تعتمد الجهة على منهجيات علمية لتحديد وتقييم المخاطر السيبرانية.	لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
تسهم استراتيجيات إدارة المخاطر في تقليل احتمالية وقوع الهجمات السيبرانية.	لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
تساعد استراتيجيات الأمن السيبراني في ضمان استمرارية الأعمال والخدمات الحكومية.	لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
يسهم تطبيق استراتيجيات إدارة المخاطر في تعزيز أمن البيئة الرقمية للجهة.	لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
تمتلك الجهة بنية تقنية متطورة لدعم الأمن السيبراني.	لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
تستخدم الجهة تقنيات حديثة لرصد واكتشاف التهديدات السيبرانية.	لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
يتم تحديث الأنظمة الأمنية بصورة مستمرة لمواجهة المخاطر الجديدة.	لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
تسهم البنية التقنية في رفع كفاءة الاستجابة للحوادث السيبرانية.	لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
تساعد الأنظمة التقنية المتقدمة في حماية البيانات والأصول الرقمية.	لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
تسهم الجاهزية التقنية في تعزيز فعالية إدارة مخاطر الأمن السيبراني.	لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة
توفر الجهة برامج تدريبية منتظمة في مجال الأمن السيبراني للعاملين.	لا أوافق بشدة	لا أوافق	محايد	أوافق	أوافق بشدة

أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	يتم نشر الوعي بالمخاطر السيبرانية بين جميع الموظفين.
أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	يلتزم العاملون بتطبيق سياسات وإجراءات الأمن السيبراني.
أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	يسهم التدريب والتوعية في الحد من الأخطاء البشرية المرتبطة بالأمن السيبراني.
أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	تسهم استراتيجيات إدارة مخاطر الأمن السيبراني في تعزيز فعالية إدارة المخاطر في الجهات الحكومية بالمملكة العربية السعودية في ضوء التحول الرقمي.

<https://forms.gle/j9NFKpQPNT3٢٤aBRGA>

Abstract

This study aimed to identify the effectiveness of cybersecurity risk management strategies in Saudi Arabian government entities in light of digital transformation. It measured the impact of implementing cybersecurity risk management strategies, technological readiness and cybersecurity infrastructure, and cybersecurity awareness and training on enhancing the effectiveness of cybersecurity risk management within these entities. The study employed a quantitative approach, using a questionnaire as the primary data collection tool. The questionnaire was administered to a sample of ٢٦٢ participants working in government entities related to cybersecurity, information technology, and risk management. The data were then analyzed using appropriate statistical methods to test the study hypotheses and achieve its objectives. The results showed a statistically significant positive impact of the independent variables on enhancing the effectiveness of cybersecurity risk management. The study also revealed that implementing risk management strategies was the most influential factor, followed by the level of technological readiness and cybersecurity infrastructure, and then security awareness and training programs. The findings confirmed that the integration of administrative, technical, and human aspects contributes to enhancing the readiness of government entities to confront cyber threats, strengthening data protection and the continuity of digital services, and supporting the success of digital transformation programs. The study recommended the continuous development of cybersecurity risk management strategies, investment in upgrading security infrastructure, expansion of training and awareness programs, implementation of international frameworks and standards in risk management, and increased use of smart technologies in threat detection. It also recommended conducting periodic assessments to measure the effectiveness of security controls and improve them to keep pace with technological advancements and evolving cyber threats.

Keywords: Cybersecurity, Cybersecurity Risk Management, Digital Transformation, Government Entities, Technical Readiness, Security Awareness, Kingdom of Saudi Arabia

Midocean University

College of Management

Master's Degree in Risk Management



**The Effectiveness of Cybersecurity Risk Management Strategies in Saudi Arabian Government Entities
in Light of Digital Transformation**

Prepared by the student/

Mishari Ali Al-Arini

University ID/

٢٥٣...١١٥

Supervisor/

Prof. Faisal Abdul Hamid

Prof. Fayez Jarad

Year

٢٠٢٦