insights

المرونة التشغيلية تحت إطار عمل الأمن السيبراني الصادر عن البنك المركزي السعودي

لماذا أصبح نضج الأمن السيبراني أولوية على مستوى مجلس الإدارة للمؤسسات المالية

انتقل الأمن السيبراني من بند في قسم تقنية المعلومات إلى أحد أجندة مجالس إدارات البنوك والشركات المالية السعودية – لأسباب محددة، مدعومة بأرقام خاصة بالسعودية

www.insightss.co/ar

الضغط التنظيمي تشدد ولم يخف

رفع تحديث إطار عمل الأمن السيبراني من البنك المركزي السعودي لعام ٢٠٢٦ مستوى الصرامة بشكل كبير: أصبح ضمان الموردين من طرف ثالث الآن إلزاميا بدلا من الاستشارات، ويجب على مؤسسات الفئة الأولى تقديم تقارير إلى مجالس إدارتها حول الأمن السيبراني مرتين في السنة بدلا من مرة واحدة. كما توافق الإطار مع ضوابط الأمن السيبراني الأساسية للهيئة الوطنية للأمن السيبراني، مما سد الفجوات التي كانت تسمح سابقا بتجاوز الممارسات الأضعف

المال على المحك – بشكل مباشر وغير مباشر

- ضمانات من طرف ثالث
- تقوم مجالس الإدارة بتقديم تقاريرها مرتين سنوياً
- التوافق مع الضوابط الأساسية للهيئة الوطنية للأمن السيبراني

المال على المحك – بشكل مباشر وغير مباشر

الأثر المالي

٤.٨٨$ مليون	٢٠ مليون ﷼	٢٥ مليون ﷼
متوسط تكلفة الاختراق	العقوبات في عام ٢٠٢٥	الغرامات التنظيمية

حجم الهجمات يستمر في الارتفاع

سجلت القطاعات السعودية – وعلى رأسها المالية والحكومة والطاقة – أكثر من ١١٠ ملايين هجوم إلكتروني في السنوات الأخيرة، وشهد عام ٢٠٢٥ وحده عمليات كشف عن هجمات فدية على بنوك الخليج، وقوائم على الإنترنت المظلم لبيانات حسابات البنك السعودية، و هجوم حجب الخدمة الموزع على مواقع البنوك

خيوط متصاعدة

+١١٠مليون
الهجمات الإلكترونية

برامج الفدية

حجب الخدمة الموزّع
الهجمات

تسريبات
البيانات

يستجيب السوق وفقا لذلك

ومن المتوقع أن ينمو سوق الأمن السيبراني في السعودية من حوالي ٤.١٩ مليار دولار في عام ٢٠٢٥ إلى ٩.١١ مليار دولار بحلول عام ٢٠٣٢ – وهو مؤشر على أن المؤسسة تتعامل مع هذا كاستثمار رأسمالي مستمر، وليس كحل لمرة واحدة

ضغط الانتظام

التأثير الصافي: فشل أمني في بنك سعودي اليوم ليس مجرد حادثة تقنية معلومات – بل هو حدث تنظيمي ومالي وسمعي يقع مباشرة على أكتاف مجلس الإدارة، مدعوما بمتطلبات حوكمة إلزامية (استراتيجية معتمدة من المجلس، استقلالية مسؤول أمن المعلومات المركزية، مؤشرات أداء قابلة للقياس) بدلا من اقتراحات أفضل الممارسات

أربع أولويات لتعزيز المرونة التشغيلية

جعل المرونة السيبرانية مسؤولية حوكمية

يجب دمج المرونة التشغيلية ضمن حوكمة الشركات بدلا من إدارتها فقط كمبادرة تقنية معلومات. يجب على المجالس والإدارة التنفيذية مراجعة المخاطر السيبرانية، وقدرات الصمود، والتقدم في المعالجة بانتظام كجزء من الرقابة الاستراتيجية الأوسع

قياس النضج، وليس فقط الامتثال

تحقيق الحد الأدنى من المتطلبات التنظيمية هو مجرد نقطة البداية. يجب على المؤسسات وضع أهداف نضج قابلة للقياس، ومراقبة مؤشرات الأداء الرئيسية ومؤشرات المخاطر الرئيسية ، واستخدام نتائج التقييم لدفع التحسين المستمر بدلا من تمارين الامتثال السنوية

دمج الأمن السيبراني مع إدارة المخاطر المؤسسية

لا يمكن للأمن السيبراني أن يعمل بشكل مستقل عن المخاطر التشغيلية، واستمرارية الأعمال، ومخاطر الطرف الثالث، وحوكمة التكنولوجيا. يمكن دمج هذه التخصصات الإدارة من فهم كيف يمكن أن تؤثر الأحداث السيبرانية على الخدمات التجارية الحيوية والمرونة التنظيمية بشكل عام

بناء ثقافة التحسين المستمر

تقوم المنظمات ذات النضج الأعلى بتقييم فعالية الضوابط، وتتعلم من الحوادث، وتجري اختبارات منتظمة، وتقوي المرونة من خلال الحوكمة المستمرة بدلا من المشاريع لمرة واحدة. هذا التحول من الامتثال التفاعلي إلى التحسين المستمر هو سمة مميزة للمنظمات الناضجة تحت صندوق الكفاءة التعاونية السامية

كيف تساعد إنسايتس المؤسسات المالية

نحن في شركة إنسايتس للاستشارات المالية والإدارية نساعد المؤسسات المالية على تجاوز الامتثال التنظيمي من خلال تعزيز قدراتها التشغيلية على الصمود من خلال

- تقييمات نضج المؤسسة بموجب إطار عمل الأمن السيبراني الصادر عن البنك المركزي السعودي
- مراجعات حوكمة الأمن السيبراني
- تقييمات المرونة التشغيلية
- تكامل إدارة المخاطر المؤسسية
- مراجعات استمرارية الأعمال وإدارة الأزمات
- تقييمات المخاطر من طرف ثالث
- استشارات حوكمة الأمن السيبراني لمجلس الإدارة والإدارة التنفيذية

يجمع نهجنا بين الحوكمة والخبرة التنظيمية وممارسات إدارة المخاطر لمساعدة المؤسسات على بناء نماذج تشغيلية مرنة تتماشى مع توقعات البنك المركزي التنظيمية

الخلاصة الأساسية

مع استمرار القطاع المالي في السعودية في تحوله الرقمي، أصبحت المرونة التشغيلية قدرة استراتيجية أكثر منها التزاما تنظيميا. المؤسسات التي تقيس وتقوي وتدمج نضج الأمن السيبراني باستمرار في حوكمة المؤسسات ستكون في وضع أفضل لإدارة الاضطراب، والحفاظ على ثقة أصحاب المصلحة، ودعم النمو المستدام

الروابط المراجع

- مبالغ الغرامات النظامية (نظام مكافحة الجرائم المعلوماتية، نظام حماية البيانات الشخصية، هيئة الاتصالات والفضاء والتقنية)
  CMS Law: Data protection and cybersecurity laws in Saudi Arabia
- حجم الهجمات (أكثر من ١١٠ ملايين هجمة)
  CYFIRMA: Cyber Threat Landscape Report – Saudi Arabia
- حوادث محددة في عام ٢٠٢٥ (هجوم حجب الخدمة الموزّع على أحد البنوك الخاصة، وقوائم بيانات الحسابات المصرفية المعروضة على الويب المظلم)
  MarkNtel Advisors: Saudi Arabia Cyber Security Market Size & Outlook
- توقعات حجم السوق (٤,١٩ مليار دولار في عام ٢٠٢٥ ← ٩,١١ مليار دولار بحلول عام ٢٠٣٢)

تمت مراجعته ومقارنته مع تقدير مستقل صادر عن

from Market Report Analytics: Saudi Arabia Cybersecurity Market 2025-2033

والذي يقدّر حجم المشاريع بنحو ١,٩٧ مليار دولار لعام ٢٠٢٥ – إلا أن التقريرين يختلفان في تحديد حجم السوق للسنة الأساسية، لذلك يُفضّل التعامل مع أرقام حجم السوق كمؤشرات تقريبية وليست أرقامًا دقيقة

2026

Insights

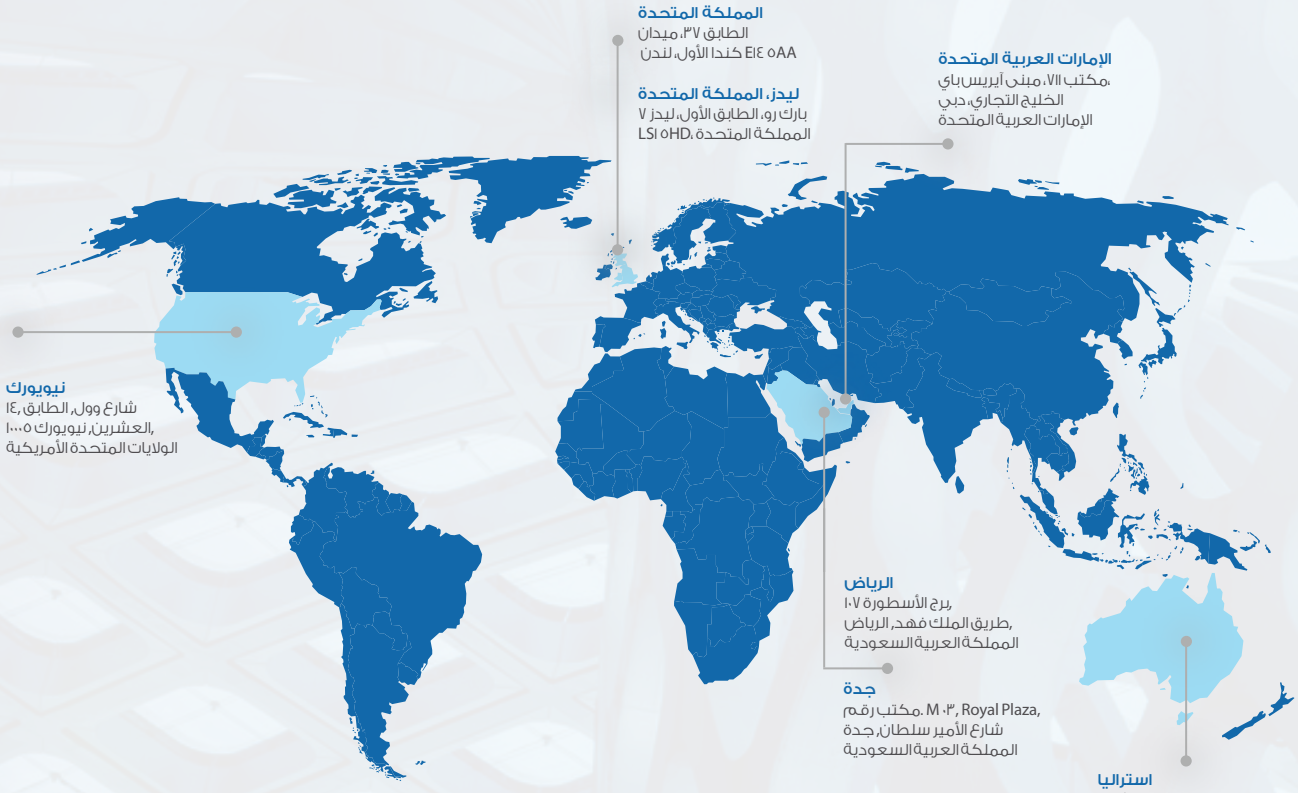
تواصل معنا

لمزيد من المعلومات والتوضيح والمناقشة بشأن المحتويات، يرجى الاتصال

خواجه سوها بت
شريك - الإستشارات المالية
sbutt@insightss.co

نيك ويتفورد
نائب الرئيس اول– لنمو اعمال
nwhitford@insightss.co

أمير عباس
نائب الرئيس – الاستشارات المالية
aabbas@insightss.co



Insights

: +966 53 775 0075
: info@insightss.co
: www.insightss.co/ar