CONCEPT

حوكمة الأمن السيبراني وإدارة المخاطر السيبرانية للقيادات التنفيذية ومجالس الإدارة

16 - 20 Aug 2027

دبي - فندق خمس نجوم في وسط الأعمال

حوكمة الأمن السيبراني وإدارة المخاطر السيبرانية للقيادات التنفيذية ومجالس الإدارة

المرجع: 1255_7501 التاريخ: 16 - 20 Aug 2027 الموقع: دبي - فندق خمس نجوم في وسط الأعمال الرسوم: SAR 19500

العمق التقني: مفاهيمي · أسلوب التطبيق: دراسة حالة

مقدمة

أصبحت الحوادث السيبرانية توقف العمليات وتفرض التزامات إفصاح وتؤثر في قيمة الأسهم، ومع ذلك ما زالت مجالس إدارة كثيرة تتلقى تقارير تقنية لا تستطيع البناء عليها. وتعتمد ميزانيات الأمن دون رغبة معلنة في المخاطر، وتبقى المسؤوليات بين القيادة التنفيذية ووظيفة الأمن وجهات التأكيد غير واضحة. تمكن هذه الدورة من كور كونسبت القيادات التنفيذية من توجيه المخاطر السيبرانية والإشراف عليها بوصفها مخاطر مؤسسية، باستخدام أطر حوكمة معتمدة ومعلومات مخاطر كمية. ويدرس المشاركون حالات من قطاعات متعددة، ويخرجون بحزمة حوكمة المخاطر السيبرانية جاهزة لمجلس الإدارة أو اللجنة التنفيذية.

أهداف الدورة

- تقييم نضج حوكمة الأمن السيبراني في المؤسسة باستخدام وظيفة الحوكمة في NIST CSF 2.0 ونموذج خطوط الدفاع الثلاثة
- توجيه حوكمة المخاطر السيبرانية من خلال ISO/IEC 27014 وCOBIT 2019 ومبادئ إشراف مجالس الإدارة المعتمدة
- تحديد الرغبة في المخاطر السيبرانية وتفسير معلومات المخاطر الكمية لترتيب أولويات الاستثمار الأمني
- مساءلة الإدارة عن مخاطر الأطراف الثالثة وهجمات الفدية والتأمين والتقنيات الناشئة
- تحديد لوحة المعلومات والمؤشرات ودورة التقارير التي يحتاجها المجلس لإشراف فعال
- اعتماد حزمة حوكمة المخاطر السيبرانية التي توضح المسؤوليات وصلاحيات القرار

الفئة المستهدفة

- أعضاء مجالس الإدارة ولجان المراجعة والمخاطر المشرفون على المخاطر السيبرانية
- الرؤساء التنفيذيون والمديرون العامون المسؤولون عن صمود المؤسسة
- رؤساء تقنية المعلومات والتحول الرقمي والتقنية الموجهون للاستراتيجية التقنية
- رؤساء المخاطر والامتثال والشؤون القانونية المسؤولون عن دمج المخاطر السيبرانية في إدارة المخاطر المؤسسية
- رؤساء أمن المعلومات الذين يرفعون تقاريرهم إلى اللجان التنفيذية ومجالس الإدارة
- الرؤساء الماليون ورؤساء العمليات الذين يعتمدون الاستثمار الأمني ونقل المخاطر

محاور الدورة

اليوم الأول: المخاطر السيبرانية بوصفها مخاطر مؤسسية

- إحاطة المجلس بالتهديدات باستخدام ملفات الخصوم في MITRE ATT&CK
- دمج المخاطر السيبرانية في ISO 31000:2018 وإطار COSO ERM
- تصميم المسؤوليات وفق نموذج خطوط الدفاع الثلاثة من IIA وخطوط ارتباط رئيس أمن المعلومات
- خط أساس نضج حوكمة الأمن السيبراني باستخدام وظيفة الحوكمة في NIST CSF 2.0
- مقارنة أنظمة الإفصاح والصمود: NIS2 وDORA وقواعد الشركات المدرجة

اليوم الثاني: أطر الحوكمة ومبادئ الإشراف

- عمليات الحوكمة في IEC/ISO 27014:2020 حوكمة أمن المعلومات: التقييم والتوجيه والمتابعة والتواصل
- أهداف الحوكمة والإدارة في COBIT 2019: EDM03 وAPO12 وAPO13
- دليل ISA-NACD لأعضاء المجالس في الإشراف على المخاطر السيبرانية: مبادئ الإشراف الستة
- مبادئ المنتدى الاقتصادي العالمي لحوكمة مجالس الإدارة للمخاطر السيبرانية
- ميثاق حوكمة الأمن السيبراني واختصاصات اللجان

اليوم الثالث: توجيه قرارات المخاطر السيبرانية

- بيان الرغبة في المخاطر السيبرانية وحدود تحملها
- القياس الكمي للمخاطر السيبرانية بنموذج FAIR
- سجل المخاطر السيبرانية المؤسسية والخريطة الحرارية وفق IEC/ISO 27005:2022
- مبررات الاستثمار الأمني: خفض المخاطر مقابل كل وحدة إنفاق
- مؤشرات المخاطر الرئيسية وتصميم لوحة معلومات الأمن السيبراني للمجلس

اليوم الرابع: التعرضات والأزمات والمخاطر الناشئة

- الإشراف على مخاطر سلاسل الإمداد السيبرانية وفق NIST SP 800-161 Rev. 1
- تقييم التأمين السيبراني وقرارات نقل المخاطر
- قرارات أزمة هجوم الفدية: الدفع والإفصاح والموازنة في التعافي
- الإشراف على مخاطر الذكاء الاصطناعي وفق IEC/ISO 42001:2023
- تقييم الثقافة الأمنية ومؤشرات نهج القيادة

اليوم الخامس: دراسات الحالة وحزمة حوكمة المخاطر السيبرانية

- دراسة حالة في الخدمات المالية: إشراف المجلس بعد تسرب بيانات العملاء
- دراسة حالة في التصنيع: توقف العمليات وحوكمة التعافي
- معايرة الرغبة في المخاطر السيبرانية لمؤسسة المشارك
- إعداد مسودة حزمة حوكمة المخاطر السيبرانية
- مساءلة من لجنة تنفيذية والدفاع عن حزمة الحوكمة

المهارات المكتسبة

- الإشراف على المخاطر السيبرانية
- تحديد الرغبة في المخاطر
- فهم القياس الكمي للمخاطر السيبرانية
- ترتيب أولويات الاستثمار الأمني
- تصميم هياكل الحوكمة
- اتخاذ القرار في الأزمات
- تقييم تقارير المجلس

لماذا تحضر هذه الدورة

- تعود بحزمة حوكمة المخاطر السيبرانية جاهزة للعرض على مجلس الإدارة أو اللجنة التنفيذية
- تطرح الأسئلة التي تكشف الافتراضات الضعيفة في التقارير الأمنية ومقترحات الاستثمار
- تميز القرارات السيبرانية التي تعود إلى المجلس من تلك التي تعود إلى الإدارة التنفيذية
- تختبر رؤيتك أمام قيادات من قطاعات ودول مختلفة تواجه تعرضات مماثلة

الخاتمة

تحسن حوكمة المخاطر السيبرانية حين يحدد القادة رغبة واضحة في المخاطر، ويسندون المسؤوليات، ويتلقون معلومات قابلة للتنفيذ. تنتقل هذه الدورة من وضع المخاطر السيبرانية ضمن إدارة المخاطر المؤسسية، مرورا بأهم أطر الحوكمة ومبادئ إشراف المجالس، وصولا إلى القرار المبني على القياس الكمي ومخاطر سلاسل الإمداد وهجمات الفدية والتقنيات الناشئة. ويخرج اليوم الأخير بحزمة حوكمة يعود بها المشارك إلى مجلسه، فيمتلك أساسا قابلا للدفاع عنه في توجيه المخاطر السيبرانية والإشراف عليها.