JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة متقدمة في قيادة الأمن السيبراني لمجالس الإدارة

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة متقدمة في قيادة الأمن السيبراني لمجالس الإدارة

قيادة الأمن السيبراني لمجالس الإدارة دورة تدريبية متقدمة مدتها أسبوعين لرؤساء أمن المعلومات ومديري التقنية والتنفيذيين غير التقنيين المساءلين أمام المجلس عن المخاطر السيبرانية، وتنتهي بخارطة طريق لاستراتيجية الأمن السيبراني على ثلاثة آفاق. فالمجالس باتت ترى الاختراق الكبير حدثا يمس استمرارية الأعمال والسمعة لا خللا تقنيا، ولذا تنعكس جودة القيادة الأمنية على القيمة السوقية والثقة. وتقدم جوبيتر برايم للتدريب هذه الدورة للقادة الذين يحملون هذه المساءلة.

لماذا تهم قيادة الأمن السيبراني لمجالس الإدارة الآن

تعيد ثلاث فئات تشكيل هذا الدور: أعضاء مجالس يتوقعون شرح التعرض السيبراني بلغة مخاطر الائتمان والسوق نفسها، وشركات تأمين ومستثمرون يسعرون الوضع الأمني للمنشأة قبل التعهد المالي معها، ومهاجمون يوقتون الابتزاز مع إعلان النتائج أو صفقات الاندماج. القائد الذي يحدد شهية مخاطر واضحة ويمول الضوابط وفقها يبقي الحوادث محصورة والإفصاح منضبطا، ومن يغفل ذلك يواجه خسائر مفاجئة وتراجعا في الثقة. وتستند الدورة إلى إطار NIST CSF 2.0 2.0 NIST Cybersecurity Framework الذي تضع وظيفة الحوكمة فيه المخاطر السيبرانية داخل استراتيجية المنشأة، وتستعين بالمعيار ISO/IEC 27001:2022 لبنية نظام الإدارة.

المستفيدون من قيادة الأمن السيبراني لمجالس الإدارة

- رؤساء الأمن الذين يضعون الاستراتيجية السيبرانية ويدافعون عن ميزانيتها أمام اللجنة التنفيذية
- مديرو التقنية الذين يوازنون بين سرعة التحول الرقمي ونطاق الضوابط
- أعضاء لجان المخاطر والتدقيق الذين يساءلون الإدارة عن التعرض السيبراني
- التنفيذيون التشغيليون المالكون لخدمات الأعمال التي يعطلها الهجوم
- الرؤساء الماليون والقانونيون الذين يقدرون التأمين السيبراني والإفصاح والمسؤولية

تجني اللجنة التنفيذية الفائدة الكبرى حين توفد رئيس الأمن مع قادة المالية والشؤون القانونية والعمليات، لأن خارطة الطريق تحتاج إلى توافق هذه الوظائف على شهية المخاطر.

قدرات قيادة الأمن السيبراني لمجالس الإدارة

يغادر المشاركون قادرين على تحويل وقائع التهديدات والضوابط إلى خيارات يستطيع المجلس اعتمادها وتمويلها ومتابعتها.

- حساب التعرض للمخاطر السيبرانية ماليا بالتقدير القائم على السيناريوهات — قرارات شهية المخاطر في المجلس
- مواءمة الاستراتيجية الأمنية مع أولويات الأعمال وخطط الاستثمار الرقمي — الرئيس التنفيذي ومكتب الاستراتيجية
- الموازنة بين خيارات الإنفاق على الوقاية والكشف والتعافي — موافقة اللجنة المالية
- تصميم هياكل الحوكمة ومواثيق اللجان وصلاحيات القرار للمخاطر السيبرانية — أعضاء المجلس ولجنة التدقيق
- تطبيق روتين قيادة الأزمات أثناء الاختراق الكبير — فريق الأزمة التنفيذي والاتصال المؤسسي
- إيصال الوضع السيبراني بمقاييس وسرد موجز للمجلس — الأعضاء المستقلون والمستثمرون

مصطلحات قيادة الأمن السيبراني لمجالس الإدارة الأساسية

- شهية المخاطر السيبرانية — مقدار ونوع الخسارة السيبرانية الذي يقبله مجلس الإدارة سعيا لتحقيق أهداف المنشأة.
- تقدير المخاطر السيبرانية كميا — التعبير عن الخسائر السيبرانية المحتملة بنطاقات مالية لمقارنتها بالمخاطر والاستثمارات الأخرى.
- الوضع الأمني — القوة الإجمالية لدفاعات المنشأة وقدرتها على الكشف والتعافي في لحظة معينة.
- وظيفة الحوكمة — الجزء من NIST CSF 2.0 الذي يحدد الاستراتيجية السيبرانية والأدوار والسياسات والرقابة ضمن إدارة مخاطر المنشأة.
- مؤشر المخاطر الرئيسي — مقياس ينبه مبكرا إلى ارتفاع التعرض مثل الأنظمة الحرجة غير المحدثة أو الحسابات المميزة دون مراجعة.
- المرونة السيبرانية — قدرة المنشأة على إبقاء خدماتها الحرجة عاملة أثناء الهجوم واستعادتها سريعا بعده.

قيادة الأمن السيبراني لمجالس الإدارة يوما بيوم

اليوم 1: نظرة المجلس إلى التعرض السيبراني

- واجبات أعضاء المجلس والرقابة السيبرانية — المساءلة على مستوى المجلس
- دوافع الجهات المهاجمة ونماذج أعمالها — التعرض حسب القطاع
- المخاطر السيبرانية في سجلات مخاطر المنشأة — المقارنة مع المخاطر الرئيسية الأخرى
- توقعات المستثمرين وشركات التأمين — إشارات تؤثر في التقييم والتغطية
- التقييم الذاتي للقيادة — الفجوات الحالية في الرقابة الأمنية

اليوم 2: أطر الرقابة التنفيذية

- وظيفة الحوكمة في NIST CSF 2.0 — توقعات الاستراتيجية والأدوار والرقابة
- ملفات NIST CSF ومستوياته — طموح الحالة المستهدفة
- بنية نظام الإدارة في ISO/IEC 27001:2022 — التأكيد المقدم لأعضاء المجلس
- نموذج الخطوط الثلاثة للأمن السيبراني — الفصل بين الملكية والمساءلة
- معايير اختيار الإطار — الملاءمة لحجم المنشأة وقطاعها

اليوم 3: تحديد شهية المخاطر السيبرانية

- بيانات شهية المخاطر — مستويات التحمل للخدمات الحرجة
- تقدير الخسائر بالسيناريوهات — حالات الفدية وسرقة البيانات والاحتيال
- أساليب التقدير الكمي للمخاطر السيبرانية — نطاقات مالية لدعم القرار
- تحديد الأصول الجوهرية — أولويات الحماية أمام المجلس
- إجراءات قبول المخاطر والاستثناءات — من يعتمد التعرض المتبقي

اليوم 4: بناء الاستراتيجية الأمنية

- مقابلات المواءمة مع الأعمال — ربط الضوابط بالإيرادات والعمليات
- تقييم نضج القدرات — خط الأساس مقابل الملف المستهدف
- مبادئ انعدام الثقة — توجه البنية المعمارية للقيادة
- بوابات الأمن في التحول الرقمي — مقايضة السرعة بالضبط
- محفظة المبادرات الاستراتيجية — التسلسل عبر ثلاثة آفاق

اليوم 5: قرارات التمويل والاستثمار

- معايير ميزانية الأمن ومحركاتها — الدفاع عن الإنفاق أمام المالية
- حالات العائد على الاستثمار الأمني — ترتيب المقترحات المتنافسة
- خيارات البناء أو الشراء أو الإسناد — بدائل خدمات الأمن المدارة
- استراتيجية التأمين السيبراني — الاحتفاظ والتغطية والاستثناءات
- الدين التقني والأنظمة القديمة — الإحلال مقابل الضوابط التعويضية

اليوم 6: هياكل الحوكمة وصلاحيات القرار

- مواثيق المجلس واللجان — موقع الرقابة السيبرانية
- خيارات خط تبعية رئيس أمن المعلومات — الاستقلالية مقابل التأثير
- هرمية السياسات واعتمادها — الملكية التنفيذية للمعايير الداخلية
- الرقابة على الأطراف الثالثة وسلسلة الإمداد — توقعات العقود والتأكيد
- المواهب الأمنية والتعاقب الوظيفي — عمق الصف القيادي

اليوم 7: قيادة الأزمات في الاختراق الكبير

- تصميم فريق الأزمة التنفيذي — الأدوار والصلاحيات والتصعيد
- إطار قرار دفع الفدية — العوامل القانونية والأخلاقية والتشغيلية
- التواصل مع أصحاب المصلحة والإعلام — توقيت الإفصاح ونبرته
- تفعيل استمرارية الأعمال — أولويات الخدمات أثناء الهجوم
- محاكاة أزمة على مستوى المجلس — القرارات في ظل معلومات ناقصة

اليوم 8: رفع تقارير الوضع السيبراني إلى المجلس

- مقاييس المجلس ومؤشرات المخاطر الرئيسية — إشارات قابلة للتصرف
- سرد الوضع السيبراني — تحويل النتائج التقنية إلى أثر على الأعمال
- خرائط التأكيد — التدقيق الداخلي والاختبار الخارجي والشهادات
- الخرائط الحرارية مقابل التقارير الكمية — اختيار الصيغة المناسبة
- حالات تقارير المجالس في المصارف والطاقة — دروس قطاعية

اليوم 9: الثقافة والتأثير والمخاطر الناشئة

- قيادة الثقافة الأمنية — نبرة القمة والمساءلة
- أساليب التأثير التنفيذي — كسب الدعم دون التخويف
- مخاطر الذكاء الاصطناعي والأتمتة — تعرض جديد في الخطط الاستراتيجية
- العناية الواجبة السيبرانية في الاندماج والاستحواذ — حماية قيمة الصفقة
- سيناريوهات الاضطراب الجيوسياسي وانقطاع الإمداد — اختبارات ضغط الاستراتيجية

اليوم 10: ممارسة خارطة طريق استراتيجية الأمن السيبراني

- تطبيق شهية المخاطر على منشأة حالة — مستوى التحمل لكل خدمة
- ترتيب المبادرات وتوزيع الميزانية — خطة آفاق ممولة
- تصميم الحوكمة والتقارير — ميثاق اللجنة ومجموعة المقاييس
- بروفة العرض أمام المجلس — مساءلة الأقران حول الوضوح والطلب
- استكمال خارطة طريق استراتيجية الأمن السيبراني — المبادرات والمالكون والمراحل

تطبيق قيادة الأمن السيبراني لمجالس الإدارة بعد الدورة

- صياغة بيان شهية المخاطر السيبرانية لأهم ثلاث خدمات حرجة وعرضه على لجنة المخاطر للمناقشة
- استبدال تقرير الأمن الحالي المرفوع للمجلس بسرد للوضع في صفحة واحدة ومجموعة قصيرة من مؤشرات المخاطر الرئيسية

أسئلة حول قيادة الأمن السيبراني لمجالس الإدارة

ما قيادة الأمن السيبراني لمجالس الإدارة ولماذا تهم الآن؟

قيادة الأمن السيبراني لمجالس الإدارة هي ممارسة تحديد شهية المخاطر السيبرانية وتمويل الدفاعات والإشراف على الأمن على المستوى التنفيذي. وتهم الآن لأن الاختراقات تمس التقييم والتأمين والثقة، وأعضاء المجلس مطالبون بإظهار رقابة مستنيرة.

من يستفيد أكثر من دورة قيادة الأمن السيبراني لمجالس الإدارة؟

يستفيد أكثر رؤساء الأمن ومديرو التقنية وأعضاء لجان المخاطر والتنفيذيون التشغيليون. وتزداد فائدتك إن كنت تعتمد ميزانيات الأمن أو ترفع تقارير التعرض السيبراني أو ستقود القرارات أثناء اختراق كبير.

كيف تختلف دورة قيادة الأمن السيبراني لمجالس الإدارة عن دورة إدارة الأمن التقنية؟

تركز الدورة على القرارات والتمويل والرقابة بدلا من إعداد الضوابط أو تشغيلها. فأنت تعمل على شهية المخاطر والتقدير الكمي وتصميم الحوكمة وتقارير المجلس، وتترك العمق التقني للدورات المتخصصة.

ماذا تعود به من دورة قيادة الأمن السيبراني لمجالس الإدارة؟

تعود بخارطة طريق تربط المبادرات الأمنية بأولويات الأعمال وشهية المخاطر. وتضم المبادرات الممولة ومالكيها ومراحلها والمقاييس التي سيتابع بها المجلس التقدم.

قيادة الأمن السيبراني لمجالس الإدارة: الطريق إلى الأمام

توجه خارطة طريق استراتيجية الأمن السيبراني أولا اختيار المبادرات التي تمولها دورة الميزانية التالية والمخاطر التي يقبلها المجلس رسميا. ويتولى رؤساء الأمن تحديثها، وينفذ المالكون التنفيذيون مبادراتها، ويتابعها أعضاء المجلس بمقاييس ربع سنوية. وبعد أول مراجعة في المجلس تستحق بيانات شهية المخاطر إعادة نظر، لأن أسئلة الأعضاء تكشف عادة أين ضبط التحمل بتساهل أو تشدد.