BLACKBIRD FOR TRAINING

إدارة مخاطر الأمن السيبراني للمديرين التنفيذيين

UK Traininig

PARTNER

www.blackbird-training.com

إدارة مخاطر الأمن السيبراني للمديرين التنفيذيين

مقدمة

في ظل التحول الرقمي المتسارع الذي يشهده العالم، أصبحت إدارة مخاطر الأمن السيبراني مسؤولية استراتيجية تقع على عاتق القادة والمديرين التنفيذيين. لم يعد الأمن السيبراني مجرد شأن تقني، بل أصبح أحد أعمدة استدامة الأعمال وحماية السمعة المؤسسية. فكل قرار تنفيذي اليوم — من الاستثمارات الرقمية إلى التحول السحابي — يحمل في طياته مخاطر سيبرانية يجب تقييمها وإدارتها بذكاء وفعالية.

تهدف هذه الدورة إلى تمكين المديرين التنفيذيين وقادة المؤسسات من فهم البنية الشاملة لمخاطر الأمن السيبراني وكيفية دمجها ضمن استراتيجيات الحوكمة المؤسسية. من خلال دراسة منهجية متكاملة، تجمع الدورة بين الإطار الاستراتيجي والإدارة العملية للمخاطر لضمان اتخاذ قرارات مستنيرة مبنية على الوعي الأمني والمعرفة الفنية الكافية.

تركز الدورة على تطوير قدرة المشاركين على تحليل التهديدات الرقمية، تقييم الأثر المالي والعملياتي لأي اختراق محتمل، وبناء ثقافة أمن سيبراني مستدامة داخل المؤسسة، مما يعزز من جاهزيتها في مواجهة التحديات المستقبلية.

أهداف الدورة

بنهاية الدورة، سيتمكن المشاركون من:

- فهم المفاهيم الأساسية لإدارة مخاطر الأمن السيبراني.
- تحديد وتقييم المخاطر التي تواجه المؤسسة من منظور استراتيجي.
- دمج إدارة المخاطر في قرارات القيادة العليا وخطط الأعمال.
- تطوير سياسات فعالة للحوكمة والأمن السيبراني المؤسسي.
- تحليل الأثر المالي والتشغيلي للهجمات الإلكترونية.
- الإشراف على بناء استراتيجيات استجابة فعالة للحوادث الأمنية.
- تعزيز التواصل بين الفرق التقنية والإدارية لإدارة المخاطر بشكل تكاملي.
- ضمان الامتثال للمعايير واللوائح الدولية الخاصة بالأمن السيبراني.

محاور الدورة

اليوم الأول: مقدمة في الأمن السيبراني وإدارة المخاطر

- المفهوم الحديث للأمن السيبراني ودوره في استدامة الأعمال.
- فهم دورة حياة إدارة المخاطر.
- التحديات التي تواجه المؤسسات في العصر الرقمي.
- العلاقة بين القيادة التنفيذية وإدارة الأمن السيبراني.
- نماذج الحوكمة الأمنية في المؤسسات الحديثة.

اليوم الثاني: تحديد المخاطر وتقييم التهديدات

- منهجيات التعرف على التهديدات ونقاط الضعف.
- تحليل المخاطر بناءً على احتمالية الحدوث والأثر.
- أدوات وتقنيات تقييم المخاطر المؤسسية.
- كيفية تحديد الأولويات الأمنية بناءً على السياق التشغيلي.
- دراسة حالات تطبيقية لتقييم مخاطر فعلية.

اليوم الثالث: تطوير استراتيجيات إدارة المخاطر

- تصميم إطار متكامل لإدارة مخاطر الأمن السيبراني.
- دمج إدارة المخاطر ضمن الخطط التشغيلية للمؤسسة.
- تطوير السياسات والإجراءات الوقائية والاستباقية.
- بناء فرق متخصصة لإدارة ومتابعة المخاطر.
- إدارة الموردين الخارجيين والمخاطر الطرفية.

اليوم الرابع: الحوكمة والامتثال والاستجابة للحوادث

- دور القيادة التنفيذية في وضع سياسات الأمن السيبراني.
- تطبيق أطر الامتثال الدولية مثل ISO 27001 وNIST.
- الإشراف على تنفيذ خطط الاستجابة للحوادث.
- تطوير خطة اتصالات فعالة أثناء الأزمات السيبرانية.
- المراجعة الدورية والتدقيق الأمني على الأنظمة.

اليوم الخامس: بناء ثقافة الأمن السيبراني المؤسسي

- تعزيز الوعي الأمني على مستوى المؤسسة.
- تطوير برامج تدريبية داخلية للموظفين.
- بناء ثقافة قائمة على المشاركة والمسؤولية الجماعية.
- قياس فعالية استراتيجيات الأمن السيبراني.
- تقييم الأداء العام وتحديد فرص التحسين المستقبلية.

لماذا يجب عليك حضور هذه الدورة؟ الايجابيات والسلبيات!

- تطوير فهم شامل لإدارة المخاطر السيبرانية من منظور القيادة التنفيذية.
- تحسين القدرة على اتخاذ قرارات استراتيجية مبنية على تقييم المخاطر.
- اكتساب مهارات قيادية في التعامل مع التحديات الأمنية المعقدة.
- تعزيز الثقة بين فرق الإدارة والتقنية لضمان حماية الأصول الرقمية.
- تعلم كيفية بناء سياسات أمنية مؤسسية متكاملة.
- ضمان الامتثال لأطر الأمن السيبراني الدولية.
- تحسين الجاهزية المؤسسية لمواجهة الهجمات المستقبلية.
- تقليل الخسائر التشغيلية والمالية الناتجة عن الحوادث السيبرانية.

الخاتمة

تمنح دورة إدارة مخاطر الأمن السيبراني للمديرين التنفيذيين القادة فهماً استراتيجياً عميقاً لمفهوم المخاطر في العالم الرقمي الحديث. إذ تركز على تمكينهم من قيادة منظوماتهم بثقة في بيئة تتسم بالتحديات التقنية المستمرة.

تجمع الدورة بين التفكير القيادي والتحليل العملي للمخاطر لتزويد المشاركين بالأدوات والمنهجيات التي تساعدهم على تحقيق التوازن بين الابتكار التقني والأمن المؤسسي. فهي لا تقتصر على إدارة الأزمات، بل تهدف إلى بناء منظومة استباقية تضمن استمرارية الأعمال وتحافظ على سمعة المؤسسة.

من خلال هذه الدورة، يصبح المديرون أكثر قدرة على اتخاذ قرارات مبنية على البيانات والتحليل، مما يعزز من قدرتهم على توجيه مؤسساتهم نحو مستقبل رقمي أكثر أماناً واستقراراً.