الدورة التدريبية: حماية بيانات الشركات - الدليل الشامل للمديرين التنفيذيين



14 - 18 ديسمبر 2026
الدار البيضاء
4500 € (للشخص الواحد)
Ref: #CYB3888_421213

مقدمة الدورة التدريبية / لمحة عامة:

في ظل التطور الرقمي المتسارع، أصبحت حماية بيانات الشركات تمثل أولوية قصوى للمديرين التنفيذيين الذين يدركون أن الأمن السيبراني للمؤسسات ليس مجرد قضية تقنية، بل هو جزء لا يتجزأ من الحوكمة المؤسسية واستمرارية الأعمال. هذه الدورة التدريبية مصممة خصيصًا لتزويد القادة بالمعرفة العميقة والاستراتيجيات الفعالة لتعزيز الأمن السيبراني للشركات وحماية الأصول الرقمية. ستتناول الدورة أطر عمل الأمن السيبراني، إدارة المخاطر الأمنية، والامتثال التنظيمي للبيانات. سيكتشف المشاركون كيف يمكنهم بناء ثقافة أمنية قوية داخل مؤسساتهم، وكيفية تقييم الثغرات الأمنية، ووضع خطط الاستجابة للحوادث السيبرانية. تُعد هذه الدورة أساسية لأي مدير تنفيذي يسعى لضمان أمن المعلومات الحساسة لشركته في مواجهة التهديدات السيبرانية المتزايدة. يستند المحتوى إلى أحدث الممارسات العالمية والأطر المعيارية، مع الإشارة إلى مساهمات خبراء بارزين في هذا المجال، مثل البروفيسور هوارد شميدت (Howard Schmidt)، الذي كان مستشار الأمن السيبراني للرئيس الأمريكي وله إسهامات كبيرة في استراتيجيات الأمن السيبراني. يقدم BIG BEN Training Center هذه الدورة بهدف تمكين القادة من اتخاذ قرارات مستنيرة بشأن أمن البيانات المؤسسية وتحقيق مرونة سيبرانية عالية.

الفئات المستهدفة / هذه الدورة التدريبية مناسبة لـ:

- المديرون التنفيذيون في مختلف القطاعات.
- أعضاء مجالس الإدارة والقيادات العليا.
- مديرو تكنولوجيا المعلومات ومديرو الأمن السيبراني.
- المسؤولون عن الامتثال وحوكمة البيانات.
- مديرو المخاطر الذين يرغبون في فهم أعمق لمخاطر الأمن السيبراني.
- المستشارون الإداريون المتخصصون في استشارات الأمن السيبراني.

القطاعات والصناعات المستهدفة:

- القطاع المالي والمصرفي لحماية بيانات العملاء المالية.
- قطاع الطاقة والبنية التحتية الحيوية لتأمين الأنظمة التشغيلية.
- الرعاية الصحية لحماية البيانات الصحية السرية.
- الاتصالات والتكنولوجيا نظرًا لطبيعة أعمالها التي تعتمد على البيانات الضخمة.
- القطاع الحكومي والهيئات العامة وما في حكمها لأمن المعلومات السيادية.
- الصناعات التحويلية التي تعتمد على البيانات التشغيلية والملكية الفكرية.

الأقسام المؤسسية المستهدفة:

- الإدارة العليا ومجلس الإدارة لوضع استراتيجيات الأمن السيبراني.
- إدارة تقنية المعلومات والأمن لتنفيذ السياسات الأمنية.
- إدارة المخاطر والامتثال لتقييم المخاطر السيبرانية.
- الإدارة القانونية لوضع السياسات والامتثال للقوانين.
- إدارة الموارد البشرية لتطوير الوعي الأمني للموظفين.

أهداف الدورة التدريبية:

بنهاية هذه الدورة التدريبية، سيكون المتدرب قد أتقن المهارات التالية:

- فهم المشهد الحالي للتهديدات السيبرانية وتأثيرها على الشركات.
- تطوير استراتيجيات فعالة لحماية بيانات الشركات ومواجهة التحديات الأمنية.
- التعرف على أطر عمل الأمن السيبراني الرائدة وتطبيقها.
- القدرة على تقييم المخاطر الأمنية ووضع خطط للتخفيف منها.
- فهم أهمية الحوكمة الأمنية والامتثال التنظيمي.
- بناء ثقافة أمنية قوية داخل المؤسسة.
- وضع خطط الاستجابة للحوادث السيبرانية وإدارة الأزمات.

منهجية الدورة التدريبية:

تتبنى هذه الدورة منهجية تدريبية تفاعلية وموجهة نحو الحلول، تضع المديرين التنفيذيين في قلب عملية التعلم. نركز على المناقشات المفتوحة، ودراسات الحالة الواقعية التي تستعرض اختراقات البيانات وكيفية التعامل معها، وتمارين المحاكاة التي تحاكي سيناريوهات الهجمات السيبرانية. سيتمكن المشاركون من تحليل أمثلة على حوادث الأمن السيبراني، وتطوير خطط استجابة عملية. يتم تشجيع العمل الجماعي لتبادل الخبرات وتطوير حلول جماعية للتحديات الأمنية المشتركة. توفر الدورة بيئة داعمة للأسئلة والنقاشات حول أفضل الممارسات في الأمن السيبراني المؤسسي. يلتزم BIG BEN Training Center بتقديم محتوى عالي الجودة يجمع بين النظرية والتطبيق العملي، مما يضمن أن يكتسب القادة الأدوات والمعرفة اللازمة لتعزيز مرونة مؤسساتهم السيبرانية. يتم التركيز على كيفية دمج الأمن السيبراني في استراتيجية العمل الشاملة لضمان استمرارية الأعمال.

خريطة المحتوى التدريبي (محاور الدورة التدريبية):

الوحدة الأولى: المشهد العام للأمن السيبراني وتحديات الأعمال

- تعريف الأمن السيبراني من منظور تنفيذي.
- التهديدات السيبرانية الحديثة التي تواجه الشركات.
- تأثير اختراقات البيانات على سمعة الأعمال وقيمتها.
- الأمن السيبراني كجزء من استراتيجية الأعمال.
- المخاطر السيبرانية على المستوى التنظيمي.
- دور القيادة في الحوكمة السيبرانية.
- أهمية تقييم المخاطر السيبرانية.

الوحدة الثانية: أطر عمل الأمن السيبراني وأفضل الممارسات

- نظرة عامة على أطر عمل الأمن السيبراني الرائدة (مثل NIST وISO 27001).
- تطبيق مبادئ الأمن السيبراني في بيئة الشركات.
- إدارة الثغرات الأمنية على مستوى المؤسسة.
- التحكم في الوصول وأمن الهوية.
- أمن سلسلة التوريد.
- أمن التطبيقات والبرمجيات.
- الامتثال لمعايير الأمن السيبراني.

الوحدة الثالثة: حماية البيانات وإدارة المخاطر

- تصنيف البيانات وحمايتها.
- سياسات حماية البيانات وخصوصية المعلومات.
- تقييم المخاطر السيبرانية وتحليلها.
- تخفيف المخاطر وبناء دفاعات سيبرانية قوية.
- النسخ الاحتياطي للبيانات وخطط التعافي من الكوارث.
- أمن البيانات في السحابة.
- حماية الملكية الفكرية الرقمية.

الوحدة الرابعة: الاستجابة للحوادث السيبرانية وإدارة الأزمات

- وضع خطة الاستجابة للحوادث السيبرانية.
- التعامل مع اختراقات البيانات والإبلاغ عنها.
- التحقيق الجنائي الرقمي الأساسي.
- التواصل أثناء الأزمات الأمنية.
- استمرارية الأعمال بعد الحوادث.
- إدارة سمعة الشركة في الأزمات.
- فرق الاستجابة للحوادث الأمنية.

الوحدة الخامسة: القيادة، الثقافة، والامتثال في الأمن السيبراني

- دور المدير التنفيذي في تعزيز ثقافة الأمن السيبراني.
- تدريب الموظفين على الوعي الأمني.
- الامتثال للوائح حماية البيانات (مثل GDPR وCCPAs).
- المتطلبات القانونية والتنظيمية للأمن السيبراني.
- إدارة أمن المعلومات كقيمة استراتيجية.
- التعاون مع خبراء الأمن السيبراني الخارجيين.
- الاستثمار في حلول الأمن السيبراني.

الأسئلة المتكررة:

ما هي المؤهلات أو المتطلبات اللازمة للمشاركين قبل التسجيل في الدورة؟

لا توجد شروط مسبقة.

كم تستغرق مدة الجلسة اليومية، وما هو العدد الإجمالي لساعات الدورة التدريبية؟

تمتد هذه الدورة التدريبية على مدار خمسة أيام، بمعدل يومي يتراوح بين 4 إلى 5 ساعات، تشمل فترات راحة وأنشطة تفاعلية، ليصل إجمالي المدة إلى 20-25 ساعة تدريبية.

سؤال للتأمل:

في عالم تتطور فيه التهديدات السيبرانية باستمرار وتصبح أكثر تعقيدًا، كيف يمكن للمديرين التنفيذيين الموازنة بين الحاجة الملحة للابتكار الرقمي والحفاظ على أقصى درجات الأمن السيبراني، لضمان النمو المستدام للمؤسسة مع حماية أصولها الرقمية بشكل فعال؟

ما الذي يميز هذه الدورة عن غيرها من الدورات؟

تتميز هذه الدورة بتركيزها الاستراتيجي الموجه خصيصًا للمديرين التنفيذيين، مما يضمن أن المحتوى يلامس التحديات الفعلية التي يواجهونها في حماية بيانات شركاتهم. نحن نقدم رؤى عميقة حول كيفية دمج الأمن السيبراني في الاستراتيجية العامة للأعمال، بدلاً من التعامل معه كمجرد مشكلة تقنية. تركز الدورة على الحوكمة السيبرانية، إدارة المخاطر على مستوى القيادة، والامتثال التنظيمي للبيانات، مما يميزها عن الدورات التقنية البحتة. نقدم دراسات حالة حقيقية لاختراقات البيانات الشهيرة، مع تحليل كيفية استجابة الشركات الرائدة لها، مما يوفر دروسًا قيمة قابلة للتطبيق. هذه الدورة لا تهدف فقط إلى تزويد المشاركين بالمعلومات، بل إلى تمكينهم من اتخاذ قرارات استراتيجية مستنيرة تساهم في تقوية الدفاعات السيبرانية للمؤسسة وتعزيز مرونتها ضد الهجمات المستقبلية.