ورشة العمل رقم (28)

أهم التحديات و المتطلبات للأمن السيبرانى لقطاع التأمين فى دولة الكويت

المحاور الرئيسية

1. أهم مخاطر و تحديات الأمن السيبرانى لقطاع التأمين

- **أهم مخاطر الأمن السيبرانى بالنسبة لقطاع التأمين :** لماذا يعتبر الأمن السيبرانى على رأس قائمة المخاطر بالنسبة لشركات التأمين ؟ و ما هى أهم العوامل التى تساهم فى إرتفاع حدة تلك المخاطر
- **تحديات الأمن السيبرانى :** لماذا يعتبر الأمن السيبرانى تحديا كبيرا لشركات التأمين ؟ و كيف يمكن للشركات مواجهة تلك التحديات بطرق عملية و فعالة

2. أهم ممارسات حوكمة الأمن السيبرانى

و يشمل هذا المحور تقديم منهجا شاملا بخطوات عملية بسيطة من شأنها إرساء قواعد حوكمة رشيدة للأمن السيبرانى فى الشركات عن طريق مناقشة النقاط التالية :

- دور مجلس الإدارة ولجانه في حوكمة الأمن السيبراني ، كيف يمكن للشركة تعزيز دور مجلس الإدارة و لجانه فى الأمن السيبرانى ؟
- بناء إستراتيجات الأمن السيبرانى ، توصيات هامة للوقوف على كيفية بناء إستراتيجية شاملة للأمن السيبرانى فى الشركة
- تقييم مخاطر الأمن السيبرانى ، التخطيط السليم للتعامل مع المخاطر السيبرانية و كيفية وضع الخطط المناسبة لمواجهة تلك المخاطر
- سياسات و أجراءات و أطر عمل الأمن السيبرانى ، توصيات هامة لوضع حجر أساس الأمن السيبرانى فى الشركة
- نشر الوعي بالأمن السيبراني على كافة المستويات فى الشركة ، أهم أدوات و طرق نشر الوعى السيبرانى
- تعزيز المرونة السيبرانية ، كيف تستطيع الشركة تعزيز قدراتها على التعافى من الأحداث السيبرانية ؟
- إدارة مخاطر الأمن السيبرانى للأطراف الخارجية ، أهم الممارسات لتقييم مخاطر الأطراف الخارجية

- توكيد الأمن السيبرانى ، كيف تتأكد الشركات من كفاءة و فعالية عمليات الأمن السيبرانى لديها ؟
- تقييم أداء الأمن السيبرانى فى الشركة ، ما هى أهم مؤشرات الأداء الرئيسية التى يمكن من خلالها تقييم أداء الأمن السيبرانى فى الشركة ؟

3. أهم الضوابط الرقابية التشغيلية للحفاظ على أمن المعلومات وسرية البيانات

و يشمل هذا المحور التوصيات المتعلقة بالحد الأدنى من الضوابط الرقابية التشغيلية للأمن السيبرانى و حماية البيانات التى يجب مراعاتها لمواجهة مخاطر الأمن السيبرانى ، منها على سبيل المثال الضوابط المتعلقة بحماية الشبكات الداخلية و مراقبة المرور الشبكى للشركة ، ضوابط حماية البيانات ، إدارة الهوية و الوصول ، إدارة الثغرات الأمنية و إختبارات الإختراق ، ضوابط إستمرارية الأعمال و التعافى من الكوارث و ضوابط إدارة الأحداث السيبرانية

4. التعامل مع الأحداث السيبرانية

يتناول هذا المحور عدة جوانب منها على سبيل المثال : ما هى الخطوات التى يجب أن تتبعها الشركة عن التعرض للأحداث السيبرانية ؟ كيف يمكن الأعداد و التجهيز للتعامل مع الأحداث السيبرانية ؟ كيف يتم الأبلاغ عن الحادث و تحليله و أحتواؤه ؟ و ما هى أهم الجوانب التى يجب مراعاتها فى خطط الأستجابة للحوادث السيبرانية ؟

عبدالرحمن محمد صبحي السيد

مدير إدارة التوكيد الرقمى | قطاع التوكيد و الخدمات الإستشارية بمجموعة الخليج للتأمين

يتولى السيد/ عبدالرحمن صبحى قيادة مهام إدارة التوكيد الرقمى بمجموعة الخليج للتأمين والمسؤولة عن التوكيد والدعم الإستشاري للأمن السيبرانى ونظم المعلومات بشركات المجموعة.

عمل السيد / عبدالرحمن مستشارا ومدققا لنظم المعلومات والأمن السيبرانى فى العديد من الشركات ومكاتب التدقيق العالمية مثل شركةIBM،Deloitte و Protiviti و التى قام خلالها بالتنفيذ والأشراف على العديد من المشروعات الإستشارية والتى تضمنت مشروعات التحول الرقمى للعديد من الشركات و التدقيق على تكنولوجيا المعلومات والأمن السيبراني (سواء تدقيق خارجى أو داخلى) ، وتنفيذ العديد من المشروعات الإستشارية المتعلقة بخطط استمرارية الأعمال و التعافى من الكوارث (BCM) وتطبيق وتقييم معايير الأيزو لأمن المعلومات ISO 27001، وتقييمات نضج الأمن السيبراني و بناء إستراتيجيات نظم المعلومات و الأمن السيبرانى للعديد من الشركات فى عدة مجالات من ضمنها التأمين و القطاع البنكى و الصناعى و الحكومى فى العديد من الدول مثل الكويت و الإمارات و السعودية و البحرين و قطر و مصر و الأردن و غيرها.

يحمل السيد / عبدالرحمن صبحى درجة البكالوريوس فى تخصص نظم المعلومات الإدارية من جامعة الإسكندرية إلى جانب دراسات عليا فى مجال تكنولوجيا المعلومات ، كما أنه حاصل على شهادة مطبِق معتمد لمعيار ISO27001 فى مجال أمن المعلومات، وشهادة مدقق معتمد لنظم المعلومات CISA إلى جانب العديد من الشهادات المهنية الأخرى.