

Un obstacle communément rencontré est de mettre en perspective son propre métier. Les fonctions de CIO et CSO ont grandement évolué en se complexifiant par la pression de diverses réglementations.

Cette complexité de fonction s'explique par le fait, qu'en plus de devoir gérer des systèmes d'information tout en maintenant le même niveau de service attendu par une organisation, le CIO et le CSO sont appelés à participer à l'élaboration des orientations stratégiques de l'organisation de l'entreprise ; tout en devant respecter le cadre légal et réglementaire.

Ces nouveaux challenges soulèvent de nombreuses questions juridiques relatives aux mécanismes technologiques, contractuels ou organisationnels.

Cette formation s'adresse aux CIO et CSO souhaitant trouver des réponses à leurs problématiques opérationnelles et leur communication sur le sujet sensible du droit et de la sécurité des systèmes d'information. Elle s'adresse également aux auditeurs informatiques et à toute personne sensible aux enjeux organisationnels et juridiques induits par l'usage extensif d'un système d'information.

OBJECTIFS :

- Se familiariser au droit appliqué aux systèmes d'information et appréhender les dernières mises à jour légales
- Trouver des réponses à des problématiques opérationnelles et intégrer une méthode de communication sur des sujets sensibles
- Cibler le discours des CIO & CSO afin qu'il soit compréhensible pour les responsables de la finance et du *compliance*
- Découvrir quelques scénarios pratiques

DUREE : 8h00

NIVEAU : tout public

Le séminaire est animé par **Nicolas Rosenthal**, expert juridique qui dispose d'une vaste expérience tant de la conformité de systèmes d'information que de la Gouvernance d'entreprise.

L'ETUDE ROSENTHAL est un Cabinet juridique de conseils dans le domaine de la gouvernance d'entreprise et la conformité réglementaire des systèmes d'information. Nous vous accompagnons dans les défis posés par l'environnement réglementaire grâce à l'analyse liée aux lois émergentes, à l'usage des technologies et à l'impact sur votre entreprise.

PROGRAMME :

8H15 LES MISSIONS DES CIO & CSO FACE AU DROIT

- Mettre en relief la valeur ajoutée du CIO/CSO dans une démarche de conformité réglementaire du système d'information
- Formaliser les missions du CSO face aux exigences réglementaires
- Permettre de changer l'image de la sécurité afin qu'elle soit vue comme une valorisation de la conformité réglementaire et non comme une contrainte.

Etablissement et mise à jour des « Chartes de sécurité »

- Principes juridiques et méthodologies
- La « Charte de Sécurité » à l'épreuve de la réalité
 - Le contrôle des communications électroniques
 - La politique de détection par
 - les traces ;
 - la responsabilité de l'utilisateur
 - les indicateurs comportementaux
 - les tableaux de bords
- La politique d'archivage des traces
 - L'intégrité des données et des personnes
 - L'organisation de la preuve

Les participants étudieront les conditions de l'utilisation des données de surveillance

Etablissement et mise à jour des Politiques techniques de sécurité

- Le fondement et les bénéfices d'une Politique technique de sécurité
- Le modèle SKIP : Security Knowledge In Practice
- La classification des systèmes : ECID-ECIA (Exposition, Confidentialité, Intégrité, Disponibilité) face au SCI (Système de Contrôle Interne)
- Exemple de structure d'une Politique technique de sécurité

Les participants étudieront des exemples de règles et de recommandations

Le management des logs

- La politique de gestion des logs
- Rôles et responsabilités
- Périmètre de la gestion des logs
- Format des enregistrements
- Protection et rétention des logs
- Habilitation des accès

Les participants étudieront la complémentarité de la gestion des logs face à un IDS (Intrusion Detection System)

12H15 Pause

14H00 LA MISSIONS DES CIO & CSO CONFRONTEE A DES PROBLEMES OPERATIONNELS

Informations sur l'organisation, le contenu du séminaire
Email : secretariat@e-droit.ch

L'externalisation des services IT

- Outsourcing : quelles limites ?
- La sélection d'un fournisseur
- Les enjeux à la fin du contrat d'externalisation
- Le cas particulier de l'Outsourcing bancaire *Circ. FINMA 2008-07*

Les participants étudieront le cahier des charges et des exemples de clause d'un contrat d'externalisation *offshore* d'un système d'information:

- Exigences générales
- Exigences détaillées
- Niveaux de services attendus

Le déploiement de services autour d'une PKI

- Les enjeux juridiques et techniques
- La gestion sécurisée de certificat
- Les infrastructures nécessaires
- Les applications sujettes à cohabitation avec une PKI : *login* réseau, signature et chiffrement, accès à distance, WiFi, applications web...
- Les étapes organisationnelles du déploiement d'une PKI selon le droit suisse et communautaire

Les participants étudieront les problématiques des listes de révocation, de la suppression du login mot de passe réseau et l'extension de la période d'expiration du mot de passe

La sécurité confrontée à la mobilité

- Les enjeux juridiques et techniques pour la sécurité
- Les principes de base et la politique
- La décomposition de la chaîne de mobilité
- La politique de sécurité des Smartphones et autres medias

Les participants étudieront la limitation des risques liés à la mobilité

18H00 Clôture du séminaire par la remise d'une attestation de formation