En collaboration avec

EM Strasbourg BUSINESS SCHOOL

Nouveau

Formation Continue
Université de Strasbourg

Cybersécurité et protection des données personnelles

Comprendre les enjeux économiques, juridiques et techniques

PERSONNES CONCERNÉES

Chefs d'entreprise, directeurs d'établissement, personnels de mairie, fonctions cadres, fonctions supports, et responsables communication / digital / marketing.

PRÉ-REQUIS

La participation à cette formation ne nécessite pas de prérequis spécifiques au regard du public auquel elle s'adresse.

PRÉSENTATION ET POINTS FORTS

Plus que jamais omniprésente, la menace cyber est en constante évolution et concerne désormais tous les types de structures, dans tous les secteurs d'activité. Au cœur de ce risque, le vol et la compromission des données économiques et des données personnelles collectées et traitées par les structures apparaissent désormais comme l'objectif prioritaire - et financier - des cyberattaquants. Cybersécurité et protection des données personnelles ne peuvent donc plus s'analyser ni s'envisager l'une sans l'autre : les législateurs européens et français l'ont compris, le cadre légal évolue et se renforce (RGPD, NIS 2, Dora, CRA...) au même titre que la responsabilité des entreprises, des administrations, et de leurs représentants légaux. Afin de connaître et prévenir le risque, il est devenu essentiel de se former, et de former ses équipes à ces enjeux.Points forts de la formation :

> **Une formation accessible aux non-techniciens / non-informaticiens**
> **Des méthodes et outils pratiques à implémenter directement dans sa structure**
> **Des analyses de cas pratiques et témoignages de chefs d'entreprises**
> **Des données actualisées grâce au recoupement de sources multiples**
> **L'analyse du cadre légal complet pour comprendre et situer son propre niveau de responsabilité**

COMPÉTENCES À L'ISSUE DE LA FORMATION

> Comprendre et expliquer l'état de la cybermenace en France et dans l'Union Européenne.
> Évaluer et calculer les coûts (directs et indirects) d'une cyberattaque pour sa structure.
> Comprendre, identifier, et distinguer les principaux risques et vecteurs d'attaques cyber au sein de sa structure et auprès des tiers (fournisseurs, prestataires, clients, etc.).
> Identifier et comprendre le rôle et les compétences des acteurs de la cybersécurité et de la protection des données personnelles au sein, et à l'extérieur de sa structure.
> Connaître et transmettre dans la pratique les règles de base de la « cyberhygiène » et de la mise en conformité au RGPD. Analyser ses propres pratiques et celles de ses collaborateurs en la matière.
> Comprendre et connaître le cadre légal général de la cybersécurité et de la protection des données personnelles.
> Analyser l'étendue de ses propres obligations et de sa responsabilité au regard de la directive européenne « NIS 2 » et du RGPD.

PROGRAMME

Jour 1

> Introduction : la cybersécurité, un enjeu économique
> Contextualisation
> Données et études 2024
> Le coût de la cybersécurité
> Faire face à une cyberattaque d'ampleur : étude de cas pratiques récents et témoignage vidéo d'un dirigeant d'entreprise.

Jour 2

> La cybersécurité et la protection des données personnelles mises en lien : aspects techniques
> Explorer les différents domaines de la cybersécurité
> Comprendre la nature de la menace
> Comprendre les conséquences de la menace
> Les acteurs, leurs rôles, leurs compétences

Jour 3

> Suite : la cybersécurité et la protection des données personnelles mises en lien : aspects techniques
> Mesures essentielles de protection
> Réagir à une cyberattaque.
> Cybersécurité et protection des données personnelles, les nouveaux enjeux légaux
> Collecte, traitement et exploitation des données personnelles
> Sécurité des systèmes d'information
> Créer sa propre veille
> Discussions de fin de stage : j'analyse mes propres pratiques et mon niveau de risque juridique.

MÉTHODES ET RESSOURCES PÉDAGOGIQUES

La formation alterne méthode explicative avec des études de cas nombreuses, des travaux pratiques une projection vidéo et des échanges avec les stagiaires. Le plan et le support pédagogique projeté seront remis aux participants.

RESPONSABLE SCIENTIFIQUE

Laura GEORG SCHAFFNER, enseignant-chercheur en marketing et systèmes d'information, EM Strasbourg.

ANIMATION

Laura Petiot, juriste, formatrice, cheffe d'entreprise et chargée d'enseignement à l'Université de Bourgogne et de Franche-Comté en cybersécurité et protection des données personnelles. Spécialiste sur les sujets liés à la cybersécurité, à l'intelligence artificielle et à la blockchain.

INTER ENTREPRISES

Durée : 3 jours (2 + 1)

En 2025
Référence SGI24-1645A
du 13 au 14 mars 2025
et le 17 mars 2025

Tarif
1490 €
Repas de midi pris en charge par les organisateurs.

Lieu
Université de Strasbourg - Service Formation Continue
21 Rue du Maréchal Lefebvre
67100 Strasbourg

STAGE INTRA : NOUS CONSULTER

Renseignements et inscriptions
Sandra GRISINELLI
Tél : 03 68 85 49 98
Sauf le jeudi après-midi et le vendredi
s.grisinelli@unistra.fr

Nature et sanction de la formation
Cette formation constitue une action d'adaptation et de développement des compétences.
Elle donne lieu à la délivrance d'une attestation de participation.
Une évaluation en fin de formation permet de mesurer la satisfaction des stagiaires ainsi que l'atteinte des objectifs de formation (connaissances, compétences, adhésion, confiance) selon les niveaux 1 et 2 du modèle d'évaluation de l'efficacité des formations Kirkpatrick.