

Former les cadres aux futurs métiers du management de la cybersécurité

L'École de Guerre Économique (EGE) fête cette année son quart de siècle. Cela fait donc 25 ans qu'elle enseigne à ses étudiants comment collecter, traiter et diffuser les informations qui peuvent être exploitées par les acteurs économiques en utilisant que des informations en sources ouvertes.



Charles Pahlawan
Directeur Adjoint de l'EGE

C'est ce qui distingue l'intelligence économique de l'espionnage économique. Le but étant qu'une information stratégique et utile reçue au bon moment par la bonne personne permette à l'entreprise d'obtenir un avantage compétitif qui peut être décisif. Et cela est surtout vrai dans les industries de l'armement, fortement compétitives et très sujettes au lobbying politique intense.

Pour Christian Harbulot, directeur de l'EGE, « l'intelligence économique se définit comme la recherche et l'interprétation systématique de l'information accessible à tous, afin de décrypter les intentions des acteurs et de connaître leurs capacités. »

Un acteur de l'intelligence économique doit maîtriser la veille et l'influence, doit fournir des aides à la décision et protéger les informations.

« L'EGE propose depuis 5 ans un MBA Executive d'un an dans le Management de la Cybersécurité et Gouvernance des Systèmes d'Information (MACYB) »

C'est sur ce dernier point : protéger les informations, que l'EGE innove. « Nous avons vécu depuis 30 ans une révolution numérique avec le développement d'Internet, sans formation réelle des salariés sur les enjeux et les risques d'un tel outil », dit Charles Pahlawan, directeur adjoint de l'École. « Certes, les gens sont désormais à l'aise dans l'utilisation basique du réseau, mais la méconnaissance de l'architecture du Net, des problématiques de propriétés de l'information et des principes de base de la cybersécurité empêchent une exploitation plus stratégique » souligne-t-il.

« Si les directions sûreté / sécurité, les risks managers sur l'évaluation des risques assurantielles... ont toujours prouvé leurs efficacités, il devient plus complexe d'évaluer le risque lié au numérique, dans nos sociétés où tout se digitalise au sein des organisations. Il convient désormais d'armer son activité d'un service spécialisé dans la gestion des risques globaux » explique M. Pahlawan.

Pour renforcer l'approche risque, gouvernance et enjeux cyber des cadres en entreprise, l'EGE propose depuis 5 ans un MBA Executive d'un an dans le Management de la Cybersécurité et Gouvernance des Systèmes d'Information (MACYB).

C'est une formation pour des cadres avec un minimum de trois ans d'expérience professionnelle, qui veulent, soit évoluer vers les nouveaux métiers liés aux risques, soit se doter de nouveaux savoir-faire pour être plus performant dans leur carrière ».

« Les 320 heures de cours sont dispensées trois jours par mois (dont un samedi) et 3 semaines bloquées pour ne pas trop impacter l'activité professionnelle du salarié en entreprise. Par notre position dominante sur le marché de l'intelligence économique, nous avons la chance d'avoir les meilleurs professionnels pour enseigner les



disciplines liées au management de la cybersécurité, comme Olivier de Maisonrouge, avocat d'affaires, auteur de nombreux ouvrages et Le spécialiste du droit de l'intelligence économique qui sait traduire ses connaissances aux cadres qui ne sont pas des juristes, ou encore Fabien Renaudin, chef du bureau Management des Risques de l'ANSSI... », ajoute le directeur adjoint de l'école. « Les prérequis techniques sont faibles puisque nos enseignements ne demandent pas de savoir-faire liés à l'ingénierie de la cybersécurité, mais une curiosité, une capacité à imaginer demain et la volonté de devenir un acteur de la décision par la maîtrise des enjeux et de la gouvernance cyber. »

La formation, qui coûte 12500 € (éligible au CPF – compte personnel de formation ou avec une convention de formation de l'entreprise) est sélective, non pas sur la recherche de profils type, car justement la pluralité des parcours ou formations des individus sont une des clés du programme, mais sur la préparation du projet professionnel. L'École a non seulement un site internet riche en information sur le programme, mais surtout des centaines de travaux réalisés par les étudiants, donc certains ont été publiés par l'édition d'ouvrages (www.infoguerre.fr).

Ceux et celles qui sont acceptés pour suivre ce MBA MACYB sont évalués sur plusieurs critères : leur présentation orale individuelle d'une synthèse d'actualités géopolitique et géoéconomique mondiale ; la rédaction d'un rapport de synthèse ; la réalisation d'une cartographie des risques ; la rédaction d'un dossier d'analyse avec des préconisations stratégiques au profit de l'entreprise étudiée ; la réalisation d'une étude diligentée par une fédération ; et, finalement, la réalisation d'une étude d'audit de sécurité.

Le programme se compose de sept modules qui commencent avec **les fondamentaux** :

- ▶ un panorama des menaces numériques,
- ▶ les grands principes de la sécurité des réseaux,
- ▶ la cryptographie,
- ▶ apprendre à penser comme un attaquant et une étude du modèle Israélien de la cybersécurité.

Les étudiants apprendront dans le deuxième module **les grands principes et fondamentaux du RGPD** (règlement général de la protection des données), et **comment devenir un (ou une) délégué(e) à la protection des données**, plus connu par son acronyme anglais DPO (data

protection officer) ainsi que son rôle, ses fonctions et ses missions.

Le troisième module est un gros morceau :

- ▶ la gestion des risques cyber ;
- ▶ comment faire un audit d'un système informatique ;
- ▶ la gestion de crise ;
- ▶ les grands principes du droit appliqué aux communications électroniques, à la finance (lutte contre la fraude et le blanchiment, etc.) et à la protection des biens et des personnes.

Le quatrième module leur apprendra **comment gérer un projet d'intelligence économique** tandis que les trois autres modules se concentrent sur **la gestion des incidents, les aspects techniques de la sécurité** et leur donne une initiation au secret défense... entre autres.

« Le diplôme décerné est une certification professionnelle délivrée de niveau RNCP 7 Européen (Master Bac +5) »

Le diplôme décerné est une certification professionnelle délivrée de niveau RNCP 7 Européen (Master Bac + 5). Le RNCP est le Répertoire National de la Certification professionnelle, qui permet de répertorier toutes les formations et tous les titres certifiés par la CNCP (Commission Nationale de la Certification Professionnelle).