

[www.cybercapitalhq.com](http://www.cybercapitalhq.com)

ISO27001 certified

**Cyber Capital HQ Consulting pour une compagnie Aérienne Européenne**

**Objectifs:**

Donner aux membres de la direction de la Compagnie et de son département informatique un ensemble de pratiques fondamentales, ayant pour but d’assurer la sécurité informatique de son réseau vis-à-vis **d’attaques potentielles et menaces internes ou** externes. A l’époque du numérique, la question sur le risque d’attaque se pose d’une façon « Quand » et pas « Si ».

Par exemple, déjà cette année, 91% des entreprises ont connu un problème de sécurité informatique et les compagnies aériennes ne sont pas épargnées. Compte tenu que les attaques visent surtout les données, les compagnies aériennes sont naturellement des cibles attractives du fait des traitements des données telles que les noms, adresses, numéros de téléphones, les documents d’identités, les informations des cartes bancaires en ligne, etc.

Les mesures adéquates pour protéger ses données peuvent épargner la Compagnie des éventuelles **sanctions par la Commission Européenne**, qui pourraient désormais s’élever à 100 millions d’euros ou 5 % du chiffre d’affaires annuel global d’une entreprise lorsque celle-ci viole les règles européennes, qui deviennent depuis 2012 de plus en plus strictes afin de protéger les données personnelles des personnes. La protection des données à caractère personnel et le respect de la vie privée sont devenus des préoccupations majeures et l’une des priorités de la Commission Européenne.

La nécessité et l’obligation de préserver la société des éventuels **litiges, amendes dissuasives et sanctions y compris pénales** prévues par la Législation Française envers les personnes morales et physiques responsables, dans le cas des infractions concernant les données, traitées par la compagnie au quotidien, dans le cadre de son activité habituelle. Une éventualité, qui peut survenir au cas où les mesures de sécurité adéquates ne sont pas mise en place lors du traitement, classement, transmission ou stockage informatique des données.

**La Réputation** des sociétés touchées par des scandales liés à des « hacking » ne revient quasi jamais à sa position initiale et porte tort à son image globale. Surtout dans le cas d’une société aérienne, la confiance une fois perdue est difficilement récupérable par la suite. Un seul incident de hacking, soit externe soit interne peut toucher l’ensemble des données, ce qui est susceptible d’entrainer une avalanche de litiges et de plaintes de chaque client, dont les données étaient concernées.

**Minimiser les risques** de tout genre qui peuvent être créés par des failles dans la sécurité informatique, capables d’entrainer la perte, le vol, le sabotage ou l’utilisation impropre des données de milliers de personnes.