



## CGI Business Consulting est qualifié PASSI

CGI Business Consulting poursuit sa stratégie d'excellence et vient d'obtenir la qualification en tant que prestataire d'audit de la sécurité des systèmes d'information (PASSI).

Cette distinction atteste du respect des exigences techniques et organisationnelles spécifiées dans le Référentiel Général de Sécurité (RGS) dans le domaine des audits de sécurité des systèmes d'information. Elle a conduit à vérifier notamment :

- la protection mise en œuvre par CGI de vos données, conforme à un niveau « Diffusion Restreinte » ;
- la compétence et le savoir-faire des auditeurs en matière d'audit de sécurité des systèmes d'information ;
- la mise en place d'un système de management spécifique aux prestations d'audits, dont l'application a été validée par le certificateur LSTI.

Toute autorité administrative peut maintenant faire appel à CGI pour mener des audits de sécurité sur ses applications soumises au RGS.

La combinaison de nos différentes offres, de la gestion des risques à l'évaluation technique des systèmes critiques, associée à une couverture géographique mondiale et à la prise compte des spécificités des Opérateurs d'Importance Vitale en France, est unique sur le marché.

## Parole d'un CyberExpert



### Évitez le scénario « Ashley Madison » !

L'exemple d'Ashley Madison démontre encore une fois la complexité pour les entreprises d'évaluer et de maîtriser les impacts d'une cyberattaque. Plusieurs enseignements sont à tirer de cette affaire.

**Les communications hâtives sont dangereuses.** La technique des pirates est en général de ne diffuser initialement qu'une partie des informations volées, afin de pouvoir décrédibiliser la communication de crise « rassurante » de l'entreprise et de publier à posteriori d'autres informations volées en réponse aux premiers communiqués de presse.

**Les risques spécifiques de l'activité doivent être identifiés pour être maîtrisés.** En l'espèce, il s'agissait pour les pirates de dénoncer l'adultère en publiant les adresses des clients, mais aussi de dénoncer aux yeux du monde que le site ne respectait pas les promesses commerciales : non-suppression des profils inopérants, profils féminins fictifs, etc. Le site était donc une cible de choix pour de tels activistes, et la posture sécurité aurait dû être adaptée en conséquence.

**Une fois les données volées publiées, l'usage qui peut en être fait est incontrôlable,** comme en témoignent les personnes malveillantes qui ont récupéré les données pour en tirer parti par chantage.

Un P.-D.G. démissionné, une entreprise qui aura du mal à survivre à ce sinistre, des vies brisées, etc. Chaque jour, Internet démontre sa capacité à faire et défaire les réputations.

C'est pourquoi la surveillance par l'entreprise des informations circulant sur Internet et au sein de son système d'information devient impérative. Elle permet de maîtriser au mieux, via la cellule de crise, les impacts de ces attaques sur l'entreprise.

Thierry Jardin — Directeur des activités sécurité CGI Business Consulting

## CyberMenaces

### 5000 £ et je vous dis tout

5000 £, c'est le prix moyen d'un espion amateur. Pour ce prix, les employés des entreprises interrogées dans cette étude ont déclaré qu'ils seraient prêts à vendre des informations protégées. Ils ont même confirmé qu'ils seraient prêts à prendre le risque de perdre leur emploi et d'assumer les conséquences judiciaires.

[Lire](#)

### La place de votre P.-D.G. est en danger

Après Sony Pictures et Target, le P.-D.G. d'Ashley Madison a également quitté ses fonctions après le scandale lié à la fuite d'information. Enfin des exemples concrets et répétés qui vous permettront de convaincre votre patron d'investir dans la sécurité !

[Lire](#)

### Windows 10 : une utilisation des données personnelles largement critiquée

Depuis sa sortie auprès du grand public en juillet dernier, Windows 10 ne cesse de faire parler de lui. Cette actualité s'explique par la découverte qu'un grand nombre d'informations personnelles sont transmises par défaut à Microsoft.

[Lire](#)

Microsoft a réagi en expliquant que la politique choisie se veut être la plus transparente possible pour l'utilisateur et qu'un contrôle total lui est accordé via de simples paramètres.

[Lire](#)

### Spear phishing : le phishing indétectable

De l'union du *phishing* classique et de l'ingénierie sociale naît une menace encore plus dangereuse pour les données sensibles : le *spear phishing*. Cette méthode utilise les informations collectées sur les réseaux sociaux pour identifier les utilisateurs cibles, personnaliser l'attaque et la rendre d'une redoutable efficacité, ce qui rend le *spear phishing* quasi imparable.

[Lire](#)

### L'ubérisation n'épargne pas le cybercrime

Le fonctionnement de Tox est simple : il vous livre un *ransomware* personnalisable et prêt à l'emploi gratuitement. Son business model ? Une commission de 30% sur les rançons versées par les victimes.

[Lire](#)

## Réponses aux CyberMenaces

### Évaluez vos capacités de CSIRT

Le CREST, organisme britannique, publie un guide d'évaluation de son niveau de maturité en matière d'*Incident Response*. Sous la forme de deux fichiers Excel, vous pouvez obtenir rapidement un état du niveau de maturité de la capacité de votre organisation à détecter, qualifier et répondre à des incidents.

[Lire](#)

### CNIL : Méthode et outillage pour mener des PIA

Pour répondre aux exigences imposées par le projet de règlement européen sur la protection des données, la CNIL a publié en juin 2015 une nouvelle méthode pour mener des études d'impacts sur la vie privée. Elle se veut plus efficace, grâce à une approche par les risques, et s'appuie sur deux guides : la méthode d'étude d'impact sur la vie privée et l'outillage.

[Lire](#)

### Nouvelle version du guide des systèmes de contrôle industriels

Le NIST a publié une mise à jour du guide ICS. Cette nouvelle version présente des façons d'adapter les contrôles de la sécurité traditionnelle pour répondre aux exigences des systèmes de contrôle industriels en termes de performance, fiabilité et sécurité.

[Lire](#)

### Des messages d'avertissement inutiles ?

C'est désormais prouvé. À force de voir toujours les mêmes messages d'avertissement ou d'erreur, le phénomène de l'habitude nous force à les ignorer. Une solution : varier la taille et les couleurs pour créer un polymorphisme de message qui attirera l'attention des utilisateurs à coup sûr.

[Lire](#)

### La sensibilisation des utilisateurs est un échec !

« Utilisez des mots de passe forts ! » « Ne mettez pas trop d'informations personnelles sur les réseaux sociaux ! » Les utilisateurs n'ont pas vocation à devenir des professionnels de la sécurité. C'est aux SI d'empêcher les utilisateurs d'adopter des comportements à risques.

[Lire](#)

## CyberRèglementation

### L'ANSSI complète son guide d'homologation de sécurité

L'ANSSI a publié en juin 2014 un guide d'homologation de sécurité à destination des maîtrises d'ouvrage. Un an plus tard, l'agence étoffe sa démarche en proposant de nouveaux outils complémentaires : un inventaire des documents types et un fichier Excel d'évaluation de la démarche à adopter.

[Lire](#)

### Données à caractères personnels : négociations finales à la Commission européenne

Les négociations à la commission européenne entrent en phase finale. La protection des données à caractère personnel va être renforcée dans un corpus de règles communes aux 28 États membres. Le pouvoir de sanction des autorités nationales devrait en être accru, mais cela suffira-t-il pour rendre la CNIL assez dissuasive ?

[Lire](#)

CGI Business Consulting fait partie du groupe CGI inc, 5<sup>e</sup> plus importante entreprise indépendante de services en technologie de l'information et en gestion des processus d'affaire au monde.

CGI Business Consulting dispose notamment d'une équipe d'experts spécialisée dans le conseil aux entreprises et aux organismes publics pour les assister à lutter efficacement et globalement contre toutes les formes de cybercriminalité.

## CyberBrèves

### Plan de contrôle CNIL : Premier bilan

Près d'un an et demi après avoir adopté et publié la recommandation précisant les modalités d'utilisation des cookies et autres traceurs, la CNIL dresse un premier bilan de son plan de contrôle. Résultat : les sites web n'informent pas suffisamment leurs visiteurs.

[Lire](#)

### Les assureurs n'assurent plus

Dans une affaire récente, un assureur a refusé d'indemniser un de ses clients au motif qu'il avait négligé la sécurisation de son système d'information. Évitez cela en prenant les mesures adéquates et en souscrivant à une assurance spécialisée dans les risques liés à la cybercriminalité.

[Lire](#)

### Perte de données : que faire ?

La *Federal Trade Commission* met à disposition un guide didactique permettant à tout un chacun de connaître les démarches à suivre en cas de perte de données à caractère personnel. Une bonne initiative !

[Lire](#)

### Le sexe : un appât qui fonctionne toujours

AdultPlayer et PornDroid sont deux applications récentes qui se font passer pour de simples applications de consultation de contenu pornographique. En réalité, ce sont des *ransomware*. Le premier prend le contrôle de l'appareil photo pour faire chanter l'utilisateur. Pour le deuxième, c'est le code de verrouillage du téléphone qui est modifié. Et à chaque fois, une rançon est demandée en usurpant les couleurs du FBI.

[Lire et Lire](#)

1%

Ce sont les employés responsables de 75% des cyberattaques.

[Lire](#)

## Chez CGI Business Consulting

### CGI Business Consulting est présent aux Assises de la sécurité du 30 septembre au 3 octobre

Christophe Long, RSSI Groupe Adjoint d'Engie, accompagné de Vincent Maret, responsable des activités cybersécurité de CGI Business Consulting, présentera un retour d'expérience intitulé « S'évaluer à travers une campagne de tests d'intrusion ».

### Recrutement

CGI Business Consulting fait face à une forte croissance de son activité sécurité. Nous recrutons des consultants sécurité. [Envoyez votre candidature.](#)



Pour de l'information en temps réel, [@CGIsecurite](#) est sur Twitter

Directeur de la rédaction Jean Olive  
Comité de rédaction Geoffroy Andrieu, Thierry Jardin, Rémi Kouby, Jean Olive, Miriam Paiola  
Contact [jean.olive@cgi.com](mailto:jean.olive@cgi.com)  
© CGI Business Consulting 2015 - <http://www.cgi.fr/conseil/cybersecurite>