Sécurité numérique.

Élaborer une réponse stratégique au cyber-risque.

Combattre le cyber-risque au sein de l'entreprise n'est plus un problème concernant exclusivement les équipes de sécurité informatique de l'entreprise. C'est rapidement devenu un point récurrent de l'ordre du jour des réunions des comités exécutifs à travers le monde en raison des fortes incidences financières, ou de réputation, qu'une fuite de données peut générer sur une organisation.

Les grands titres dans les médias, comme « Cyber-attaque ! », « Grave fuite de données » et « Coup de hackers... » sont de plus en plus fréquents et les conséquences pour les organisations touchées peuvent s'avérer particulièrement coûteuses et peuvent mettre en péril leur développement.

Estimation des coûts

Les trois principales causes à l'origine d'une fuite de données sont : les attaques malveillantes ou criminelles, les dysfonctionnements du système de protection IT ou une erreur humaine[1]. Les coûts suite à une fuite de données varient selon la cause, les mesures de protection en place au moment de la détection de l'incident, le délais entre l'incident et la mise en place de ces mesures et la nature des données volées. Une récente étude gouvernementale britannique a établi que le coût moyen d'une fuite de données a plus que doublé entre 2014 et 2015 pour atteindre une fourchette moyenne comprise entre 1,46m £- et 3,14m £ pour les grandes organisations[2].

Outre les dépenses liées à la résolution des cyber-attaques, les entreprises découvrent qu'elles doivent s'engager dans des dépenses considérables pour reconstruire et regagner leur image de marque et acquérir de nouveaux clients.

91% des grandes organisations ou entreprises ont subi une violation de sécurité en 2015

50% des violations de sécurité les plus graves sont dues à une erreur humaine

28% des violations de sécurité les plus graves sont dues en partie au manque d'implication de la direction qui n'accorde pas une priorité suffisante à cette question

15% des grandes organisations ont subi une violation de la sécurité ou des données lors de la dernière année, notamment à partir de l'utilisation de smartphone ou tablette

16% ont été attaqués par une personne extérieure non-autorisée au cours de la dernière année

Source : Gouvernement Britannique - Enquête sur les violations de sécurité des informations 2015.

De plus, les cadres supérieurs sont pleinement conscients des retombées qui découlent d'une réputation entachée et de la perte de confiance de leur clientèle.

Confiance du client

Que votre client soit une entreprise ou un consommateur, il est temps de s'interroger sur leur confiance vis-à-vis de la sécurité de leurs informations qu'ils vous confient. Quelles sont les mesures que vous prenez pour les rassurer en matière d'intégrité des données et de sécurité numérique ? Comment pouvez-vous vous démarquer en tant qu'organisation qui prône l'excellence dans le domaine de la cyber-sécurité ?

[1] *Source : Enquête sur les violations de sécurité des informations 2014 – Service des Entreprises, de l'innovation et des compétences.*

[2] *Source : Gouvernement de Sa Majesté - Enquête sur les violations de sécurité des informations 2015.*

bsi.

...making excellence a habit.™

La certification de la sécurité numérique et au-delà

Chez BSI, nos experts ont des connaissances techniques pointues qui vous aideront à avoir une vue d'ensemble. Nous explorerons comment votre entreprise peut s'assurer de faire tout ce qui est en son pouvoir pour contrer le cyber-risque, nouer des liens de confiance avec les clients et mieux se démarquer des concurrents sur le marché.

Nous pouvons aider votre organisation à se conformer aux normes demandées par l'industrie, à mettre en place et appliquer les meilleures pratiques pour ainsi faire la preuve que vos systèmes sont fiables, sûrs, et garantissant un niveaux de qualité élevé. Dans le cadre de votre solution BSI Certification Numérique, nous pourrons envisager : la mise en conformité à l'ISO/IEC 27001, système de management internationalement reconnu pour la sécurité des informations, de mettre en place Les programmes Cyber Essentials et Cyber Essentials Plus norme de cyber-sécurité, la certification CSA STAR ou l'ISO/IEC 27018 qui concernent la sécurité des données dans le Cloud.

En outre, la certification BSI **Kitemark** relative à la **Sécurité numérique** et aux **Transactions numériques sécurisées** est adaptée aux organisations souhaitant démontrer un niveau d'engagement encore plus élevé en matière de sécurité digitale par rapport aux exigences des référentiels standards.

À propos de BSI Kitemark™

En 2015, une enquête de consommateurs indépendante a établi que la Marque BSI Kitemark est associée à une certaine rigueur et à une qualité de service. Les consommateurs savent que les produits et services affichant le logo BSI Kitemark sont éprouvés et testés, favorisant ainsi leur confiance.

Qu'est-ce qui explique cela ?

67%
des consommateurs **sont sensibles** au logo BSI Kitemark.

La Présence du Kitemark sur le produit pourrait justifier des **majorations de prix** jusqu'à
26%

60%
des consommateurs **prêts à payer plus** pour un produit portant le logo BSI Kitemark.

Cyber Essentials

Est une norme de cyber-sécurité identifiant les contrôles de sécurité que les organisations doivent prévoir au sein de leurs systèmes informatiques pour assurer qu'ils bénéficient d'un niveau élémentaire de cyber-sécurité et pallient les menaces Internet les plus courantes. BSI est un organisme de certification accrédité CREST associé au plan Cyber Essentials. Depuis octobre 2014, Cyber Essentials constitue une exigence minimum lors de soumissions d'offres pour certains contrats gouvernementaux* et devient une exigence obligatoire pour de nombreux autres contrats contenant des informations sensibles ou présentant un risque modéré à élevé.

ISO/IEC 27001

Correspond au système de management de la sécurité de l'information le plus reconnu au monde permettant aux organisations de protéger efficacement toutes les données financières et confidentielles et de prouver aux clients et parties intéressées que la sécurité est vitale pour leur fonctionnement. Il contribue à identifier les risques menaçant vos informations essentielles et à mettre en place les contrôles appropriés pour mieux contrer les risques.

**Reconnu par les autorités du Royaume Uni*

Sécurité numérique Kitemark

La sécurité numérique (Digital Security) Kitemark s'appuie sur les principes des Transactions Numériques Sécurisées Kitemark (Secure Digital Transactions Kitemark) avec une portée plus étendue, en mesurant la sécurité des Réseaux, Applications, Infrastructures et Opérations. Les domaines couverts sont le management des risques et de la sécurité de l'information.

Cela exige de l'organisation qu'elle couvre tout ou une partie de ces domaines selon la norme ISO/IEC 27001 et qu'elle ait pondéré les risques dans l'Annexe A de l'ISO/IEC 27001. Ces domaines sont testés sur 10 000 heures en termes de vulnérabilité, via des méthodes comme le CVSS (Common Vulnerability Scoring System) pour calculer les résultats.

Certification au-delà des normes requises

Certification CSA STAR pour le Cloud

Au vu du développement croissant de services informatiques hébergés et des nouveaux risques dans ce domaine, BSI a travaillé avec le Cloud Security Alliance (CSA) pour appliquer et développer une certification.
La CSA STAR est une garantie supplémentaire au vu des risques les plus importants dans le Cloud.

Kitemark pour la sécurisation des Transactions numériques

Le BSI Kitemark pour les transactions numériques sécurisées Secure Digital soumet un site ou une application Web à des tests stricts et indépendants sous la norme OWASP (Open Web Application Security Project) ASVS V2.0 (Application Security Verification Standard) lors de leur transit depuis un dispositif via Internet vers un serveur, en veillant ainsi à ce que les contrôles de sécurité soient en place vis-à-vis des informations financières et/ou personnelles gérées. Les hébergeurs de tout site ou application Web peuvent rassurer leurs clients sur leur sécurité en affichant le logo Kitemark sur leurs supports marketing. L'évaluation implique que les organisations atteignent et conservent la certification ISO/IEC 27001 pour les parties de l'entreprise gérant des données confidentielles tout en passant des tests de pénétration internes et externes stricts qui détectent les vulnérabilités et failles de sécurité.

ISO/IEC 27018

La norme procure des directives aux fournisseurs de services cloud qui traitent des renseignements personnels (Personally Identifiable Information - PII) et vise à traiter les risques liés au cloud computing public et favorise la confiance envers les fournisseurs de cloud computing public. Il procure un ensemble de contrôles que les fournisseurs de services cloud (Cloud Service Providers - CSP) sont tenus de mettre en place pour traiter les risques spécifiques et contient des instructions sur ce que les CSP doivent accomplir en termes d'obligations contractuelles et réglementaires.

Cyber Essentials Plus

Cela englobe tous les éléments de Cyber Essentials en plus d'une évaluation de sécurité interne des dispositifs d'utilisateur final. Il s'agit d'une évaluation plus poussée conduite par BSI, accrédité CREST, qui testera si les contrôles individuels ont été correctement mis en place en recréant divers scénarios d'attaque pour déterminer si votre système risque d'être compromis. C'est une photographie de la sécurité de votre organisation au moment de l'audit qui ne procure toutefois pas la garantie que les contrôles continueront d'être correctement mis en place ou que votre système est en mesure de se défendre contre des attaques.

À propos de BSI

Nous sommes l'organisme de normalisation qui aide les organisations à faire de l'excellence une habitude, dans le monde entier. C'est notre créneau permettre aux autres d'obtenir de meilleures performances. Avec plus de 3000 collaborateurs dans le monde, nous aidons nos clients à obtenir de meilleures performances, à réduire les risques et à assurer un développement durable.

Formée en 1901, BSI a été le premier organisme de normalisation national au monde et plus d'un siècle plus tard, est salué au plan international comme le défenseur des bonnes pratiques. BSI est à l'origine de bon nombre des normes appliquées aux systèmes de management les plus couramment utilisés dans le monde et publie plus de 2 700 normes par an. Ces normes traitent des problèmes les plus urgents à l'heure actuelle : transparence de la facturation, management de l'énergie, accès des personnes handicapées, nanotechnologies, etc. tout en couvrant des secteurs divers dont l'aérospatiale, la construction, l'énergie, l'ingénierie, la finance, la santé, l'informatique et le commerce de détail.

Les normes de BSI sont étayées par une approche collaborative et rigoureuse affinée sur des décennies en collaboration avec des experts de l'industrie, des organismes publics, des associations professionnelles, des entreprises de toutes tailles et des consommateurs, afin d'élaborer des normes d'excellence.

BSI travaille avec plus de 80 000 clients répartis dans 162 pays dans le monde pour les aider à adopter et à cultiver les habitudes de bonnes pratiques. Les clients sont formés et reçoivent des conseils pratiques pour la mise en œuvre, ainsi qu'un ensemble d'outils de mise en conformité. De plus, pour veiller à ce qu'ils reçoivent le meilleur service, BSI est également évalué de façon indépendante et est accrédité à l'international par ANAB (ANSI-ASQ National Accreditation Board) et par 26 autres organismes d'homologation dans le monde, dont UKAS (United Kingdom Accreditation Service).

L'influence de BSI est internationale et BSI joue un rôle essentiel dans l'Organisation Internationale de Normalisation (International Organization for Standardization ou ISO). En tant que membre fondateur, BSI veille à ce que les normes internationales élaborées traitent des besoins actuels et futurs des entreprises et de la société, tout en offrant de réels avantages à une organisation et à ses partenaires.

Contactez un de nos experts aujourd'hui au : **+33 (0)1 55 34 11 40**
ou visitez notre site web
www.bsigroup.fr

bsi.

BSI Group France
19 Rue Alphonse de Neuville
75017 - Paris
T: +33 (0)1 55 34 11 40
E: contact.france@bsigroup.com