bsi.

...making excellence a habit.™

# Maîtriser la VULNÉRABILITÉ

La place des normes dans l'atténuation des risques liés à la cybersécurité

# Avant-propos

**BSI s'attache à promouvoir les meilleures pratiques afin de faire face à un challenge en constante mutation : la cybersécurité. Au service d'entreprises de toute taille dans 182 pays du monde, nous favorisons la conformité, réduisons le risque et renforçons la résilience.**

Howard Kerr, Directeur Général, BSI

# Introduction

C'est à un groupe de lycéens de Chicago que l'on impute le tout premier acte de piratage de réseau jamais recensé. En 1967, les membres du club informatique du lycée Evanston Township High School s'introduisaient dans le système réseau d'IBM. Ils avaient, pour cela, utilisé les terminaux de téléimprimeurs que la société avait gracieusement offerts à l'établissement. Quelques années plus tard, Creeper, le premier virus informatique moderne, était lâché sur ARPNET, l'ancêtre d'Internet. Il se répliquait d'ordinateur en ordinateur, laissant derrière lui un bref message : « I'm the creeper, catch me if you can! » (Je suis le Creeper, attrape-moi si tu peux).

Le terme de « virus » est employé pour la première fois dans un contexte de cybersécurité en 1984, dans un article publié par l'Université de Caroline du Sud. Le concept moderne de l'impact des cyber-attaques sur la société s'est développé au cours de la décennie suivante. DEF CON, la première convention sur le piratage se tient en 1993, s'imposant rapidement comme un rendez-vous annuel très attendu en matière de cybersécurité.

Les progrès numériques s'accélèrent au cours des années suivantes et jusque dans le nouveau millénaire, au même rythme que les cyber-attaques et les vols de données. Les médias sociaux font leur apparition, les appareils mobiles se démocratisent à la maison et au travail, et le commerce électronique explose. Chaque avancée est une nouvelle brèche dans laquelle s'engouffrent les criminels, et un nouveau risque pour les utilisateurs bien intentionnés de commettre des erreurs qui coûtent cher.

En un peu plus d'une génération, la cybersécurité est passée d'un concept obscur au statut de priorité internationale. Ses implications, dans un premier temps d'ordre purement expérimental, sont devenues une question de sécurité économique et civique, voire de sûreté de l'État. Les gouvernements sont contraints désormais de protéger en permanence les infrastructures critiques connectées. La moindre faille dans les réseaux de ressources et de services vitaux peut avoir de terribles répercussions sur la vie de millions de citoyens.

Dans le contexte des entreprises, la cybersécurité a depuis longtemps cessé d'être de la responsabilité des seuls services informatique. Les activités quotidiennes de chacun sur le lieu de travail sont désormais régies et guidées par une réelle prise de conscience et les connaissances des employés. L'utilisation de normes reconnues à l'échelle internationale pour la conception des systèmes de cybersécurité et la formation des employés participent au renforcement de la protection des données et au respect des législations.

Le présent rapport revient sur quelques-unes des principales difficultés liées à la cybersécurité, soulignant l'importance des normes dans le renforcement de la résilience organisationnelle. Il aborde des aspects aussi vastes que la protection des employés qui utilisent des appareils personnels pour exécuter des tâches professionnelles ou l'établissement des normes de sécurité dans le marché émergent de l'Internet des Objets. C'est un point de départ très utile pour identifier les normes qui permettront d'optimiser votre résilience organisationnelle •

John DiMaria
Responsable Monde de la sécurité de l'information et de la continuité d'activité chez BSI Group

## Sommaire

# Mécanismes et contrôles liés aux BYOD* :
## Une approche normalisée

De plus en plus prisé, le concept du BYOD consiste pour les employés à utiliser leurs appareils personnels (ordinateurs portables, tablettes et smartphones) pour leurs activités professionnelles, se connectant aux réseaux de l'entreprise et générant ou stockant des données. Une approche normalisée permet aux entreprises d'atténuer les risques de sécurité liés aux modalités du BYOD.

Selon un rapport rédigé par MarketsandMarkets, le marché du BYOD et de la mobilité d'entreprise devrait représenter 73,3 milliards de dollars d'ici 2021[1]. Mais le BYOD ne fait pas l'unanimité – certains y voient gains potentiels de productivité et d'économie, quand d'autres sont plus sensibles aux risques de violation des données.

La mise en place par les entreprises d'une politique BYOD spécifique et élaborée conformément aux normes ISO/IEC27001 (Management de la sécurité des informations) et ISO/IEC38500:2015 (Gouvernance des technologies de l'information) est une mesure de protection élémentaire.

La sensibilisation des employés et la compréhension de ces derniers des enjeux pour la sécurité sont essentielles pour minimiser les risques organisationnels. La communication régulière des bonnes pratiques dans ce domaine, adressée à tous les collaborateurs de tous les niveaux, est importante. L'entreprise ne peut se contenter de supposer que le personnel se chargera lui-même de s'informer et de se former.

Tout le monde doit être impliqué dans le processus et être invité à s'exprimer et à émettre des suggestions. Il convient de rappeler à chacun et à intervalles réguliers les responsabilités individuelles qui l'incombent. L'idéal serait d'avoir des employés formés et proactifs, soucieux de se protéger mutuellement et de protéger les intérêts de leur entreprise, capables d'intervenir et d'encadrer les autres.

**“La sensibilisation des employés et la compréhension de ces derniers des enjeux pour la sécurité sont essentielles pour minimiser les risques organisationnels.”**

Outre favoriser l'intégration des nouvelles recrues, une politique BYOD normalisée se doit d'intégrer des procédures en cas de départ d'un employé. Cela est particulièrement important lorsque les employés ne partent pas de leur plein gré. Les entreprises peuvent exiger l'exécution de certaines actions avant le départ d'un employé, comme la suppression des fichiers, mais la procédure doit être clairement énoncée dans la politique relative aux BYOD.

Il convient également de stipuler si l'employé est digne de confiance et procèdera à l'action requise ou si le service informatique doit s'acquitter de cette tâche. Il est essentiel de suivre et d'appliquer la politique dans les plus brefs délais dès la confirmation du départ prochain d'un employé.

*BYOD = Bring Your Own Device


La probabilité d'utilisation de ses propres appareils mobiles sur le lieu de travail est élevée, ce qui accroît d'autant plus la difficulté à obtenir la restitution des données requises.

Il convient par ailleurs de prendre en considération toute modification législative, comme le Règlement Général sur la Protection des Données (RGPD) lors de l'élaboration et de la mise à jour d'une politique BYOD[2]. Soucieux de renforcer la protection des données à caractère personnel pour les résidents de l'UE, le RGPD transforme la manière dont les entreprises collectent, conservent, traitent et partagent les données.

Les politiques liées aux appareils mobiles et BYOD doivent refléter les exigences du RGPD, en particulier ce qui concerne l'accès, l'identification et la collecte des données. Le RGPD ne fait plus reposer la responsabilité sur les individus mais sur les entreprises désormais tenues de fournir les données et les fichiers exigés.

La norme BS 10012 relative au système de gestion des informations personnelles permet aux entreprises de démontrer qu'elles possèdent le niveau de compétences requis dans les domaines où le RGPD est critique. Le risque de violation de données depuis les appareils mobiles peut également être atténué à travers des applications de gestion actualisées afin de faire la distinction entre les fichiers personnels et professionnels d'un utilisateur, cependant les politiques BYOD intégrant des normes établies restent le meilleur rempart.

Le comportement des employés en dehors de leur lieu de travail habituel est un autre facteur important. Imaginons un employé utilisant un appareil mobile pour se connecter en dehors de son environnement de travail habituel. Son exposition aux menaces, telles que l'hameçonnage, s'accroît car les employés sont plus enclins à négliger les mesures de sécurité dès lors qu'ils accèdent à du contenu sans rapport avec le travail.

Le rapport de Wombat Security, intitulé « Beyond the Phish 2017 » a révélé que près d'un quart des personnes interrogées n'ont pas su répondre correctement à des questions sur la protection des appareils mobiles et des informations[3].

Enfin, lorsqu'une erreur est commise, l'éducation est essentielle, qu'elle soit dispensée en personne ou par le biais d'une application logicielle dédiée. L'adoption d'un plan d'intervention actualisé en cas d'incident permet également de clarifier immédiatement les responsabilités et de prendre les mesures adéquates pour contenir et contrôler la situation en cas de violation. Nul ne saurait trop insister sur l'importance de procéder en continu à des évaluations des risques et à des essais pour garantir la sécurité et la pertinence des politiques BYOD.

Références

1. www.marketsandmarkets.com/Market-Reports/enterprise-mobility-334.html
2. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr
3. Beyond the Phish Report 2017, publié par Wombat Security : www.wombatsecurity.com/beyond-the-phish

# L'Internet des Objets : Normes et sécurité

Tim McGarr, responsable du développement des marchés chez BSI, explique pourquoi la sécurité est essentielle à l'arrivée à maturité de l'Internet des Objets.

Si l'Internet des Objets (IoT) apporte des améliorations notables dans nos vies quotidiennes en termes d'efficacité, d'automatisation et d'optimisation globale, des efforts supplémentaires sont attendus pour développer des normes de sécurité unilatérales afin de protéger les individus, les entreprises et leurs données.

L'IoT désigne les objets connectés à Internet qui partagent indépendamment les données qu'ils collectent sur un réseau. Qu'il s'agisse de technologie portable pour le fitness capable de transmettre le rythme cardiaque et la respiration sur le cloud ou de bus communiquant avec les systèmes de trafic info dans les villes, chaque point de données collectées et mesurées contribue à une opportunité quasi infinie d'affiner, de contrôler et d'optimiser notre vie quotidienne .

Selon les prévisions, le marché de l'IoT devrait passer de 2990 milliards de dollars en 2014 à 8900 milliards en 2020, atteignant un taux de croissance annuel composé 19,92%, et promet des innovations potentiellement transformatrices. Mais de par la nature si vaste et omniprésente de l'IoT, la vulnérabilité de la cybersécurité représente un défi majeur. Imaginons une entreprise ayant plusieurs de ses systèmes connectés à Internet afin de maximiser l'efficacité à travers l'automatisation et le partage des données. Peut-être ses systèmes de chauffage, de ventilation et de climatisation, ses machines, la sécurité des bâtiments et les capteurs environnementaux sont tous reliés à l'IoT et les uns aux autres. Cette situation aggrave la complexité de la sécurité et des risques et augmente le nombre de portes dérobées ou de failles par lesquelles les hackers peuvent s'introduire dans le système.

En 2015, le réseau électrique d'Ukraine occidentale a été attaqué, laissant près de 250 000 foyers sans électricité pendant six heures. Les hackers avaient pris le contrôle du système de contrôle et d'acquisition de données et désactivé l'opération à distance[2]. Fin 2016, le logiciel malveillant Mirai avait exploité de nombreux appareils IoT vulnérables, prenant leur contrôle afin de lancer des attaques à grande échelle sur les réseaux[3].

Outre le domaine strictement numérique, les implications en termes de sécurité pour les conducteurs de véhicules connectés et autonomes durant une cyber-attaque ciblée du réseau de contrôle, voire des véhicules individuels, illustrent parfaitement nos vulnérabilités physiques.

Le marché de l'IoT doit s'accompagner de pratiques et de normes largement reconnues afin de rassurer le public. La sécurité des données collectées, partagées et traitées, ainsi que l'accès aux appareils eux-mêmes revêtent une importance particulière. Chaque mois, de nouveaux objets connectés sont commercialisés. Mais les fabricants n'ont pas tous la même approche de la sécurité. En l'absence de recommandations dans les normes comme ISO/IEC27001, il est difficile de rassurer les utilisateurs et de garantir que les mécanismes de protection et contrôle appropriés ont été appliqués lors du processus de conception des produits.

La croissance de ce marché émergent est telle que de nombreuses autres questions méritent d'être posées pour chaque appareil connecté, notamment :

- Quelles certifications de sécurité l'hébergeur de l'infrastructure cloud détient-il ?
- Le fabricant a-t-il pris les mesures adéquates pour sensibiliser les futurs utilisateurs à l'importance de la sécurité, par exemple, leur recommander de changer les mots de passe par défaut ?
- Quelle norme de cryptage des données est utilisée ? Qu'en est-il du contrôle d'accès et de l'authentification des utilisateurs ?

À cet égard, BSI fait figure de leader dans ce domaine avec la spécification PAS 212 « Signalement automatique des ressources pour l'IOT » élaborée conjointement avec l'organisation Hypercat Alliance.

Les documents PAS 182 et 183 s'y rapportent fortement. Le PAS 182 présente d'importantes considérations liées à la sécurité essentielles à la mise en œuvre des concepts de smart city, notamment l'interopérabilité des systèmes et le partage des données entre les différentes agences.

Le PAS 183 définit le cadre régissant le partage des données entre les villes, énonçant les orientations pour un usage approprié et expliquant quels types de données peuvent être publiés et partagés et quels types méritent de rester confidentiels.

Par la suite, les normes resteront un élément central régissant la manière dont les individus et les entreprises se prépareront aux risques de sécurité de l'IoT et les atténueront. La nature mondiale de sa croissance exige une approche véritablement collaborative et internationale pour l'élaboration et l'application des normes de sécurité. BSI a à cœur de créer une communauté inclusive afin de relever ce défi et d'accélérer l'adoption des normes de sécurité pour le marché de l'IoT ●

> **Le marché de l'IoT doit s'accompagner de pratiques et de normes largement reconnues afin de rassurer le public.**


Références

1. www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#9e2d8981480e
2. www.incapsula.com/blog/critical-infrastructure-cyber-security.html
3. www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/

# Cybersécurité : tendances et statistiques

## 90%

des données disponibles dans le monde ont été créées dans les deux dernières années[1].

## 54%

des travailleurs américains pensent pouvoir faire confiance aux réseaux WiFi publics dans les lieux autorisés.[2]

## Plus de la moitié

des travailleurs américains et britanniques laissent leur ordinateur portable professionnel dans la voiture quand ils vont déjeuner, au lieu de l'emporter avec eux [3].

## Un Yobioctet =

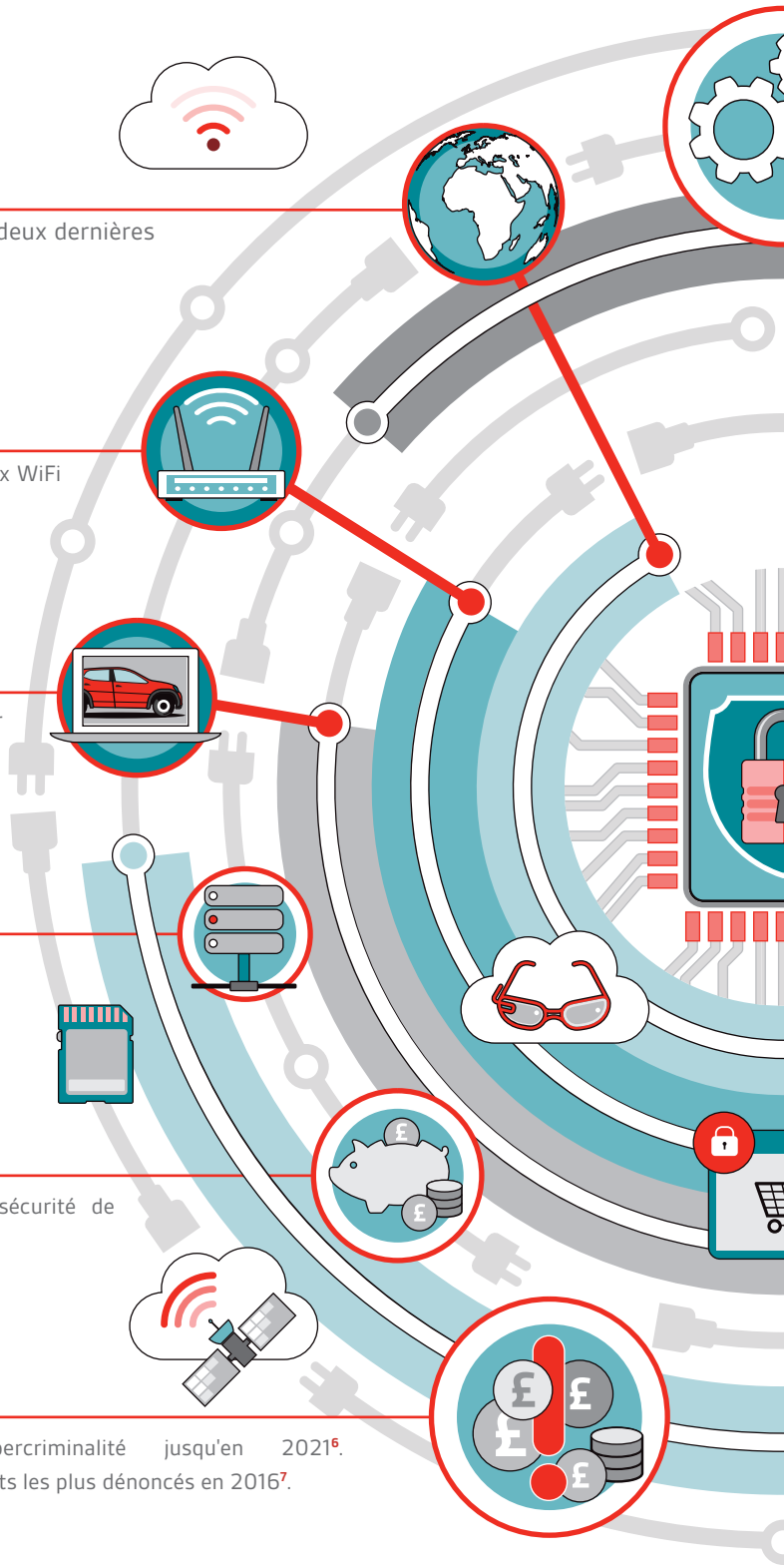
1 208 925 819 614 629 174 706 176 octets [4].

## 93 milliards de $

Dépenses mondiales projetées pour les services et produits de sécurité de l'information en 2018[5].

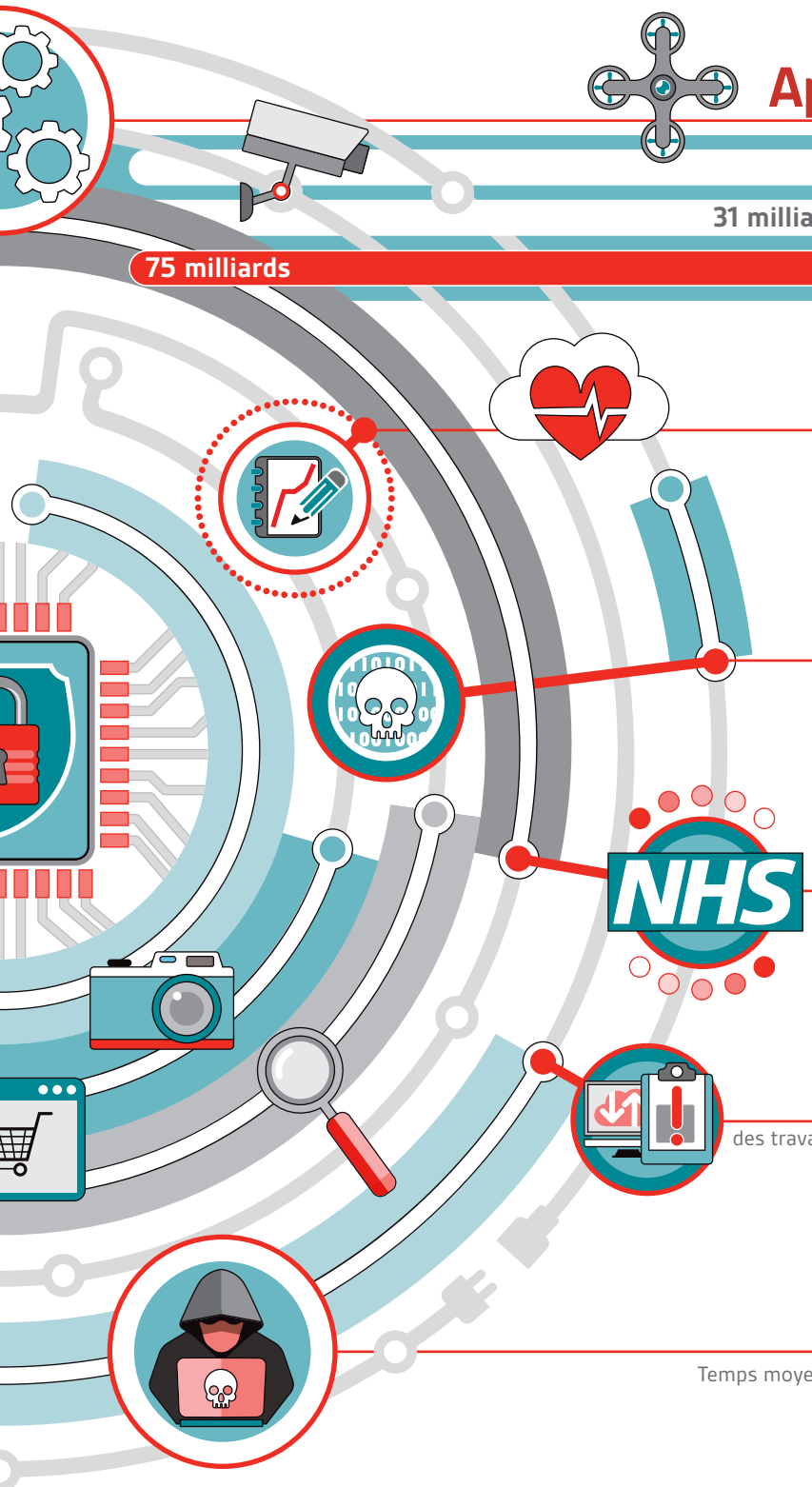
## 6 milliards de $

Coûts annuels des dégâts occasionnés par la cybercriminalité jusqu'en 2021[6].
À l'échelle mondiale, la cybercriminalité occupait la 2ème place des délits les plus dénoncés en 2016[7].



References


1. www.iflscience.com/technology/how-much-data-does-the-world-generate-every-minute/
2. 3. 12. Beyond the Phish Report 2017, publié par Wombat Security : www.wombatsecurity.com/beyond-the-phish
4. https://techterms.com/definition/yobibyte
5. www.gartner.com/newsroom/id/3784965
6. www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html




## Appareils connectés à l'IOT[8]

15 milliards 2015

31 milliards 2020

75 milliards 2025

## Près de 60

enregistrements de données sont perdus ou volés chaque seconde [9].

## Seuls 4%

des données volées étaient sécurisées, c'est-à-dire rendues inexploitables par le cryptage [10].

## 42%

des services du NHS n'ont pas mis en place le programme de cybersécurité préconisé par le gouvernement britannique et intitulé « 10 étapes vers la Cybersécurité »[11].

## 40%

des travailleurs britanniques ayant installé un VPN déclarent ne l'utiliser que rarement, voire jamais[12].

## 146 jours

Temps moyen pendant lesquels les hackers restent cachés dans un réseau[13].


7. www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html
8. www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
9. 10. https://breachlevelindex.com/
11. www.information-age.com/uks-critical-infrastructure-skipping-basic-cyber-security-checks-123468204/
13. www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics

# Cybersécurité et protection des infrastructures critiques

John DiMaria, Responsable Monde de la sécurité de l'information et de la continuité d'activité chez BSI Group, explique en quoi une approche normalisée est le meilleur rempart contre les menaces internes et externes.

Lorsqu'ils évoquent les atouts essentiels du bon fonctionnement de la société, les gouvernements désignent en général les réseaux d'électricité, de communication, de chauffage, de santé et de transport. La défaillance de l'un ou de plusieurs de ces systèmes centraux, ne serait-ce que pendant une courte période, aurait des conséquences immédiates sur la vie de millions de personnes.

Les réseaux nationaux d'infrastructure modernes sont de plus en plus interconnectés et interdépendants, partageant des données et des informations pour renforcer l'efficacité et les contrôles. Cependant, cette situation renforce la vulnérabilité du système dans son intégralité, à savoir que la moindre défaillance d'un élément particulier provoquera une réaction en chaîne sur le réseau connecté plus vaste. L'évaluation et l'atténuation continues des risques sont donc essentielles pour leur protection, en particulier du point de vue de la cybersécurité.

Les infrastructures critiques feront toujours l'objet de tentatives de cyber-attaques. Outre l'importance vitale qu'elles revêtent, les hackers sont séduits par les multiples opportunités d'infiltration qu'elles présentent. Selon une étude mondiale réalisée en 2017, 67 % des personnes interrogées ont signalé des attaques multi-vectorielles par déni de service distribué, contre 56 % en 2016.

Par ailleurs, de nombreux gros réseaux d'infrastructure ne possèdent pas la protection adéquate. En 2017, une étude portant sur 338 organisations à infrastructure critique au Royaume-Uni a montré que 42 % des services du NHS n'avaient pas mis en place le programme de cybersécurité préconisé par le gouvernement britannique intitulé « 10 étapes vers la cybersécurité » publié en 2012. En outre, plus de la moitié de ces organisations semblaient ignorer le risque d'attaques rapides et furtives de type déni de service distribué sur leurs réseaux, un type d'attaque couramment employé pour implanter des malware, des ransomware ou pour le vol de données[2].

FQui plus est, les réseaux d'infrastructure critiques dans de nombreux pays sont gérés par différentes entreprises privées travaillant toutes en étroite collaboration avec le gouvernement au niveau local, régional et national. Avec l'intervention de tant de groupes et de parties prenantes, une approche harmonisée de la cybersécurité est essentielle, reposant sur les meilleures pratiques reconnues.

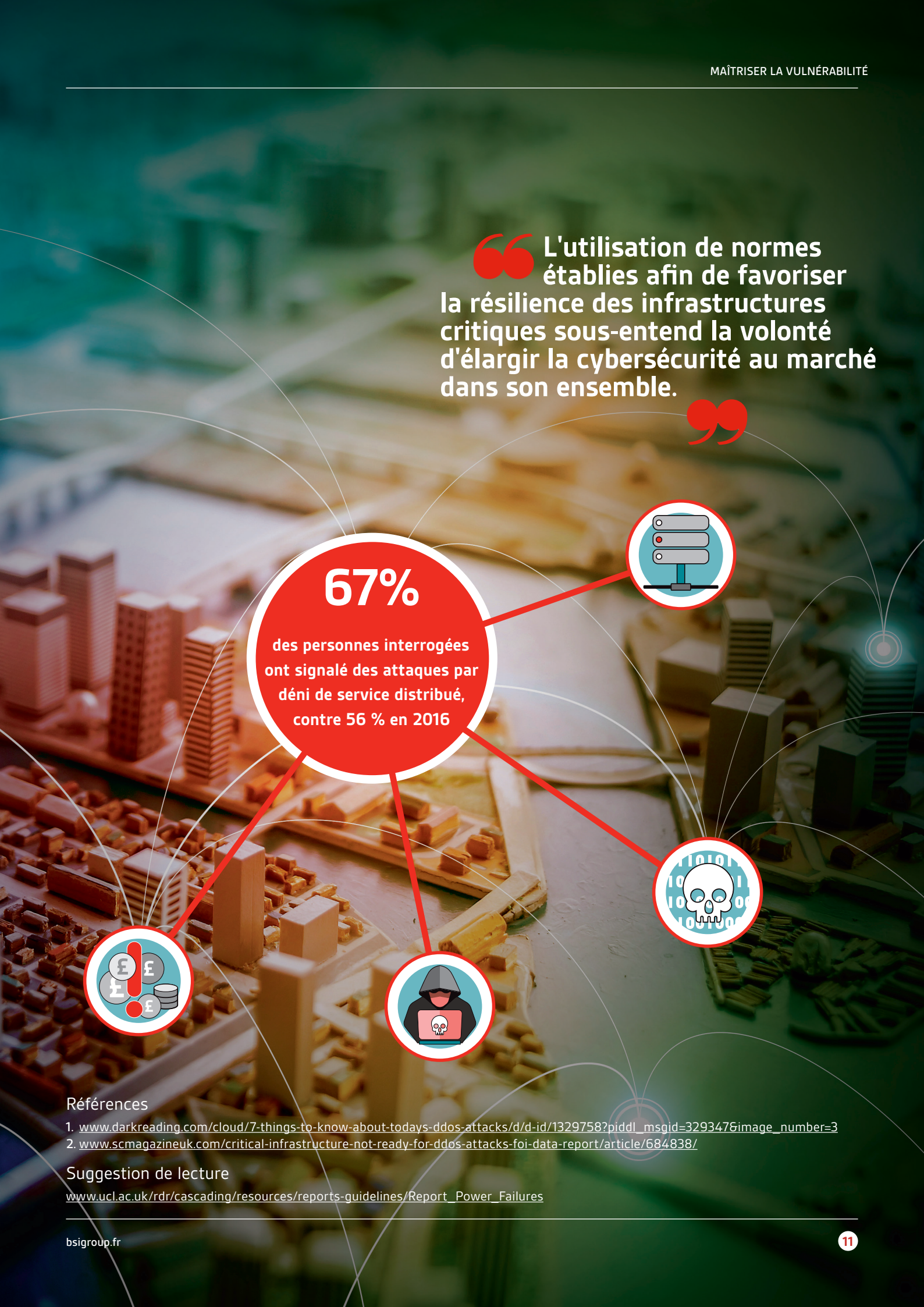
BSI organise régulièrement des réunions, des comités et des groupes de travail qui rassemblent des gouvernements et entreprises chargées de veiller à l'infrastructure critique afin de mettre en place et d'harmoniser les meilleures pratiques. C'est ainsi que la famille de normes ISO/IEC27000 a vu le jour.

Elle garantit également la mise en place des contrôles adéquats. Par ailleurs, la certification aux normes de sécurité reconnues est exigée pour les entreprises intervenant dans les chaînes d'approvisionnement des infrastructures les plus critiques. Elle permet aux éventuels partenaires de la chaîne d'approvisionnement de partager et de communiquer de manière transparente leurs garanties de sécurité et de fournir un cadre pour l'amélioration continue, les audits de contrôle qualité et les processus de validation.

Outre les cyber-attaques externes, une approche normalisée de la protection des infrastructures critiques permet également de réduire les risques associés à l'erreur humaine. À travers les formations spécialisées et les mesures d'évaluation de performance, les entreprises développent une sensibilité accrue à la sécurité qu'elles distillent à leurs collaborateurs qui maintiennent dès lors un haut degré de diligence. Par ailleurs, dans le cadre d'une enquête sur un incident de sécurité survenu, être capable de prouver que les politiques internes à l'entreprise sont conformes aux normes reconnues à l'échelle internationale, permet de réfuter les accusations de négligence.

Enfin, il convient de noter qu'il est irréaliste d'attendre des gouvernements et des législateurs qu'ils puissent isolément suivre le rythme des hackers. À ce titre, une collaboration internationale et à long terme, ainsi que l'application des normes, restent le moyen le plus efficace de protéger les infrastructures critiques et les données à l'échelle mondiale •

> **L'utilisation de normes établies afin de favoriser la résilience des infrastructures critiques sous-entend la volonté d'élargir la cybersécurité au marché dans son ensemble.**




## Références

1. www.darkreading.com/cloud/7-things-to-know-about-todays-ddos-attacks/d/d-id/1329758?piddl_msgid=329347&image_number=3
2. www.scmagazineuk.com/critical-infrastructure-not-ready-for-ddos-attacks-foi-data-report/article/684838/

## Suggestion de lecture

www.ucl.ac.uk/rdr/cascading/resources/reports-guidelines/Report_Power_Failures

# Confidentialité des données, conformité et RGPD

John DiMaria, Responsable Monde de la sécurité de l'information et de la continuité d'activité chez BSI Group, explique en quoi une gouvernance des données normalisée est le meilleur moyen d'aboutir à la conformité réglementaire.

En 2018, le Règlement Général sur la Protection des Données (RGPD) a supplanté la Directive sur la Protection des Données de 1995 qui ne suffisait plus à protéger les données à caractère personnel à l'ère des géants de l'Internet et du Cloud que sont Google et Facebook.

La législation évolue rarement au même rythme que la technologie et que les transformations sociales et commerciales qu'elle suscite. L'introduction du RGPD illustre une réelle volonté de voir la législation rattraper la technologie. Durant les années qui se sont écoulées entre l'instauration du RGPD (2011) et son entrée en vigueur (2018), l'utilisation des smartphones, la recherche vocale et l'Internet des Objets (IoT) se sont largement démocratisés. Cependant, les principes de la bonne gouvernance des données sont restés d'une pertinence rassurante, même si la complexité de la menace et les opportunités de violations des données semblent s'être renforcées.

Le RGPD prévoit des amendes et des pénalités plus lourdes en cas de non-respect, et place de manière explicite la responsabilité sur les entreprises, conférant aux citoyens et résidents de l'UE le plein contrôle de leurs informations à caractère personnel. Le RGPD est la plus importante mise à jour des lois européennes existantes sur la protection des données entreprise en si peu d'années, un événement qui a été largement couvert par les médias les mois précédent son entrée en vigueur en mai 2018.Cela étant, il convient de rappeler qu'il existe plus de 100 autres règlements territoriaux sur la protection des données, chacun s'accompagnant de ses propres exigences et dispositions. Une approche normalisée de la gouvernance des données organisationnelles est la meilleure base pour aboutir à une conformité mondiale cohérente.

L'application de normes reconnues en matière de protection des données permet aux entreprises de déterminer leurs niveaux actuels et potentiels d'exposition, et offre un cadre de contrôles destinés à les gérer ou à les atténuer. La certification atteste que les mesures de protection des données sont en place, ce qui rassure les parties prenantes et les clients. D'ailleurs, de nombreuses entreprises clairvoyantes ont profité de l'introduction du RGPD pour se démarquer et renforcer leur image d'entreprise responsable.

La norme BS 10012 aide les entreprises à définir leurs risques et exigences de conformité au titre du RGPD, puis à introduire un système de gestion des informations personnelles adapté à leur activité. Une fois le système en place, les entreprises peuvent demander une certification indépendante afin de démontrer leur bonne gestion des données à caractère personnel et l'actualisation de leurs processus dans le cadre d'une politique d'amélioration continue.

Enfin, la certification aux normes de gouvernance des données reconnues accroît la transparence entre les fournisseurs, attestant que les contrôles adéquats sont en place et réduisant les risques de mise en cause en cas d'incident •

## Cinq grandes questions à se poser et les normes qui s'y rapportent

### La norme BS 10012 aide les entreprises à gérer aux mieux les données. Elle pose cinq questions :

1. À qui appartiennent les données ?
2. Pourquoi les traitons-nous ?
3. Où sont-elles conservées ou transférées ?
4. Combien de temps les conservons-nous ?
5. Quels mécanismes de protection avons-nous mis en place ?

Les autres normes pertinentes sont, notamment, l'ISO/IEC27018 pour la protection des informations personnelles identifiables dans le cloud public, l'ISO/IEC29151:2017 qui énonce un ensemble de contrôles supplémentaires harmonisés avec l'ISO/IEC27001, la BS ISO/IEC38505-1:2017 pour la gouvernance et les contrôles des données, ainsi qu'une nouvelle norme : l'ISO/EC27552, une extension des normes ISO/IEC27001 et ISO/IEC27002 qui définit les lignes directrices relatives aux bonnes pratiques de gestion de la sécurité de l'information.

## 10 principales normes relatives à la cybersécurité

| | |
|---|---|
| ISO/IEC27001 | Management de la sécurité de l'information. |
| BS EN ISO/IEC27002:2017 | Code de bonnes pratiques pour les contrôles au sein d'un système de management de la sécurité de l'information. |
| BS ISO/IEC27003:2010 | Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information. |
| BS ISO/IEC27005:2011 | Gestion des risques liés à la sécurité de l'information. |
| ISO/IEC27017 | Contrôles de sécurité de l'information pour les services du cloud public. |
| ISO/IEC27018 | Protection des informations personnelles identifiables dans le cloud public. |
| BS ISO/IEC27031:2011 | Lignes directrices pour mise en état des technologies de la communication et de l'information pour continuité des affaires. |
| BS ISO/IEC27032:2012 | Lignes directrices pour la cybersécurité. |
| BS ISO/IEC27033-1:2015 | Sécurité de réseau. Vue d'ensemble et concepts. |
| BS ISO/IEC27034-5:2017 | Protocoles et structure de données de contrôles de sécurité d'application. |

# Qu'est-ce que le RGPD ?

Le Règlement Général sur la Protection des Données (RGPD) du Parlement Européen, du Conseil de l'Union Européenne et de la Commission Européenne vise à harmoniser et à renforcer la législation sur la protection des données sur le marché européen.

Il permet aux citoyens et résidents de l'Union Européenne (UE) de contrôler leurs données à caractère personnel, supplantant la Directive sur la Protection des Données de 1995 créée bien avant qu'Internet n'occupe une place aussi prépondérante. Le Règlement cherche également à rassurer le public concernant l'économie numérique émergente et sur la manière dont les géants modernes comme Facebook et Google collectent et utilisent les données des utilisateurs.

Si le RGPD a durci les pénalités et les amendes infligées en cas de non-conformité et de violation, il offre également aux entreprises une plus grande clarté juridique et uniformise la loi sur la protection des données au sein du marché unique[1].

Le RGPD introduit plusieurs exigences importantes, notamment des changements concernant les aspects suivants :

- Le consentement, qui doit désormais être expressément affirmé par le sujet des données et enregistré par le contrôleur des données
- Qu'est-ce qu'une donnée à caractère personnel
- Demandes d'informations sur la conservation et l'utilisation des données, délais de réponses de la part des entreprises et demande de suppression des données
- Délais et protocoles en cas de violation des données

## Responsable du traitement des données et sous-traitant des données : deux rôles distincts

Le RGPD définit deux fonctions au sein d'une entreprise : le responsable du traitement des données (appelé « contrôleur de données ») et le sous-traitant des données (appelé « processeur de données »).

Le contrôleur désigne la personne qui détermine les finalités et les moyens du traitement des données à caractère personnel. Le processeur désigne la personne ou le groupe de personnes qui traite les données à caractère personnel pour le compte du contrôleur. Les deux doivent désormais répondre aux exigences du RGPD.

Référence

1. www.eugdpr.org

**“...les principes de la bonne gouvernance des données sont restés d'une pertinence rassurante, même si la complexité de la menace et les opportunités de violations des données semblent s'être renforcées.”**

# Atténuer les risques liés à l'erreur humaine

David Maher, Directeur marketing international, BSI Cybersécurité et Résilience de l'Information, souligne les défis auxquels les entreprises sont confrontées dans le paysage numérique actuel.

L'erreur humaine fera toujours partie intégrante du profil de risque pour la cybersécurité d'une entreprise, et elle est souvent considérée comme une faiblesse potentielle. Mais avec une formation normalisée de qualité, cette faiblesse pourrait bien devenir un atout.

Les employés sont souvent cités comme étant le maillon faible de la cybersécurité, et en effet, l'erreur humaine est chaque année à l'origine d'un fort pourcentage de violations des données et de sécurité.

Les criminels cherchent souvent à exploiter les individus, plutôt que les systèmes car ils comprennent l'impact des techniques de piratage psychologique sur les individus surmenés ou distraits qui ne privilégient pas toujours la cybersécurité. Le rapport de Wombat Security, intitulé « Beyond the Phish 2017 » a révélé que près d'un quart (24 %) des personnes interrogées n'ont pas su répondre correctement à des questions relatives à l'identification des menaces d'hameçonnage. La marge de manœuvre est énorme pour les criminels à l'affût de la moindre opportunité de vol de données et d'usurpation d'identité, profitant de l'ignorance ou de la négligence des utilisateurs[1].

Plutôt que d'adopter des mesures réactives, les entreprises seraient plus avisées de faire de leurs employés un maillon fort de la chaîne de la cybersécurité, leur donnant les moyens d'agir comme un rempart humain à l'intrusion. Et cela est d'autant plus vrai avec l'essor du télétravail et l'utilisation de plus en plus fréquente des appareils mobiles personnels sur le lieu de travail à des fins professionnelles. La sensibilisation à la cybersécurité doit s'étendre au-delà de l'espace de travail habituel des employés.

À travers des simulations d'hameçonnage et d'évaluations des connaissances, les entreprises peuvent identifier avec précision les besoins spécifiques en formation et les risques réels, idéalement au niveau des utilisateurs individuels. À partir de là, les entreprises peuvent personnaliser leurs programmes de formation en fonction des besoins des employés. La norme ISO/IEC27001 de management de la sécurité de l'information aide les entreprises à créer et structurer la formation conformément aux meilleures pratiques internationales.

L'étude menée par Wombat Security révèle que l'employé moyen manque également de connaissances en matière de précautions, pourtant jugées élémentaires. À titre d'exemple, plus de la moitié des travailleurs américains pensent pouvoir faire confiance aux réseaux WiFi publics dans les lieux autorisés, 40 % des travailleurs britanniques ayant installé un VPN déclarent ne l'utiliser que rarement, voire jamais et plus de la moitié des travailleurs américains et britanniques reconnaissent laisser leur ordinateur portable professionnel dans la voiture quand ils vont déjeuner, au lieu de l'emporter avec eux. L'étude met également en avant des besoins en formation sur la sécurité physique, comme la protection d'objets tels que des badges d'identité, des données et fichiers imprimés contenant des informations confidentielles sur les fournisseurs[1].

Il convient également de s'interroger sur le format de la formation à la cybersécurité. Une formation annuelle aura moins de chances d'aboutir aux résultats escomptés ou de suffisamment sensibiliser le personnel. Nous préconisons plutôt des séances de formation brèves mais fréquentes, ainsi que le ciblage des employés afin de leur proposer du contenu pertinent. Pour favoriser un réel changement dans le comportement, il convient de créer une culture de la participation où les employés se sentent impliqués, sont invités à s'exprimer et à faire des suggestions d'amélioration.

La formation normalisée à la cybersécurité peut faire naître une réelle prise de conscience chez les employés et intégrer le concept de responsabilités individuelles et collectives à tous les niveaux hiérarchiques. S'ils cernent mieux la nature des risques, les employés sont plus à même de signaler tout agissement suspect, devenant par-là même une excellente première ligne de défense.

Il est, en outre, important d'introduire des mécanismes de signalement simples et rapides pour dénoncer les actes douteux. Les systèmes de cybersécurité les plus performants n'empêcheront pas les risques d'erreur mais leur gravité devrait être considérablement réduite.

L'application d'un plan d'intervention actualisé en cas d'incident permet également de clarifier immédiatement les responsabilités et de prendre les mesures adéquates pour contenir et contrôler la situation. Il convient de consigner les détails de l'événement à des fins d'apprentissage et d'amélioration continue. Il peut également être nécessaire de prévoir des séances de renforcement des connaissances après la survenance d'attaques ou d'événements préoccupants.

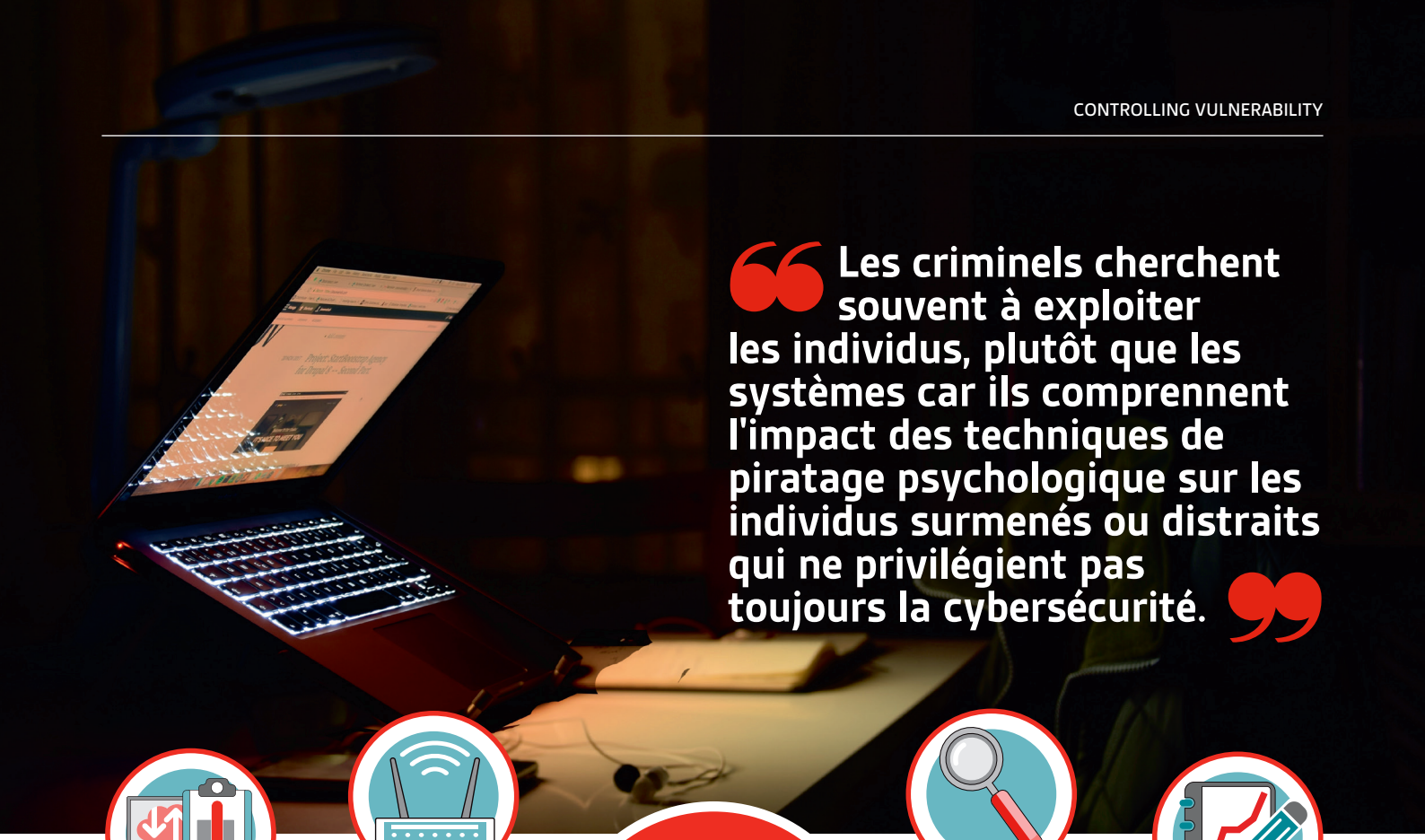
Enfin, la certification d'une entreprise attestant du respect et de l'application des normes reconnues dans ses processus et sa formation en cybersécurité est importante. En cas de violation des données, l'entreprise est en mesure de prouver qu'elle a mis en place les contrôles nécessaires pour satisfaire ses obligations de manière responsable et raisonnable ●

## Services d'intervention accrédités par CREST

Les services d'intervention proposés par BSI aident les entreprises à se préparer et à réagir efficacement aux événements de violation des données ou aux cyber-incidents. À travers les méthodologies préconisées par le SANS Institute, le NIST et la norme ISO/IEC27001, nous effectuons des essais afin de tester les systèmes et de déterminer si les processus en place sont adéquats.

Les professionnels expérimentés de BSI effectuent des exercices périodiques de « chasse aux menaces » à l'aide de logiciels et de systèmes centralisés, ou conjointement à des analyses de mémoire ciblées sur les principaux actifs. Nous procédons également à des exercices de détection des menaces en prévision d'événements organisationnels spécifiques. Par exemple, préalablement à la fusion de deux réseaux dans le cadre d'une acquisition, nous pouvons être amenés à réaliser une "chasse aux menaces" afin de déceler les éventuels signes de faiblesse.

Grâce à l'approche proactive de BSI, le personnel est en mesure d'intervenir de manière méthodique face à un incident de sécurité, selon un cadre défini. Les rôles et les responsabilités sont clairement établis afin de favoriser une intervention rapide et pertinente. Nous veillons également à ce que les obligations légales, réglementaires et contractuelles soient définies et documentées.



> **Les criminels cherchent souvent à exploiter les individus, plutôt que les systèmes car ils comprennent l'impact des techniques de piratage psychologique sur les individus surmenés ou distraits qui ne privilégient pas toujours la cybersécurité.**


Références

1. Beyond the Phish Report 2017, publié par by Wombat Security : www.wombatsecurity.com/beyond-the-phish
2. PhishMe, 2016 : www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704

# Base de données en ligne des normes de cybersécurité : BSOL

**75%**
**des entreprises pensent que la norme ISO 27001 réduit le risque encouru[1]**

La cybercriminalité coûte chaque année plusieurs centaines de milliards de dollars à l'économie mondiale. Avec BSI, vous pouvez choisir de protéger votre activité, vos employés et vos clients. Notre bibliothèque en ligne des normes (BSOL) disponible depuis le site web de BSI Group au Royaume-Uni garantit un accès instantané à la norme de cybersécurité adéquate.

L'utilisation d'informations dépassées pour protéger ses systèmes critiques peut avoir de graves répercussions. Disponible 24h/24, la BSOL permet aux abonnés de consulter et de télécharger les dernières normes en matière de cybersécurité, et de créer des alertes spécifiques et des notifications électroniques au moment des mises à jour.

## Principales normes de cybersécurité à mettre en œuvre

| | |
|---|---|
| ISO27001 : | Systèmes de management de la sécurité de l'information. La base de toute stratégie de cybersécurité efficace. |
| ISO27002 : | Technologies de l'information. Techniques de sécurité. Code de pratique pour les contrôles de sécurité de l'information. |
| ISO27003 : | Technologies de l'information. Techniques de sécurité. Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information. |
| ISO27005 : | Technologies de l'information. Techniques de sécurité. Gestion des risques liés à la sécurité de l'information. |
| ISO27017 : | Technologies de l'information. Techniques de sécurité. Code de pratique pour les contrôles de sécurité de l'information basés sur l'ISO/IEC27002 pour les services du cloud. |
| ISO27018 : | Technologies de l'information. Techniques de sécurité. Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans le cloud public public agissant comme processeur de PII. |
| ISO20000-1 : | Technologies de l'information. Gestion des services. |

**Pour bénéficier d'une démonstration ou obtenir de plus amples informations, veuillez appeler le +33 (0)1 55 34 11 40 ou écrire à l'adresse suivante contact.france@bsigroup.com**

### Référence

1. The Economic Contribution of Standards to the UK Economy Report, publié en juin 2015 par Cebr & BSI.

### Clause de non-responsabilité

# Cybersécurité : Formation et certification avec BSI

La formation du personnel aux principales normes de sécurité et de cyber-résilience, comme la norme ISO/IEC27001, est essentielle à l'application d'une politique de cybersécurité. BSI propose des formations adaptées à tous les aspects de la cybersécurité et à tous les niveaux hiérarchiques.

Après l'adoption et la mise en œuvre réussies d'une norme, la certification indépendante atteste de la volonté de votre entreprise d'offrir un service d'excellence en matière de sécurité de l'information.

## 1 Adopter les normes

L'utilisation de normes reconnues pour les processus et la planification de la cybersécurité permet aux entreprises d'affiner leur conformité et d'atténuer les risques liés à leur activité quotidienne. Les normes sont une indication de la mise en place d'opérations efficaces et durables, attestant de la qualité de vos processus, une information à laquelle vos clients et partenaires ne sont pas insensibles.

## 2 Suivre les formations

Vous venez d'introduire une norme ou souhaitez procéder à un audit pour une certification existante, BSI propose un éventail de formations adaptées à vos besoins, ainsi que des formations dédiées aux cadres dirigeants. Les formations de BSI traitent différents sujets, notamment le RGPD, la conformité en matière de sécurité de l'information ou encore la sensibilisation des utilisateurs finaux.

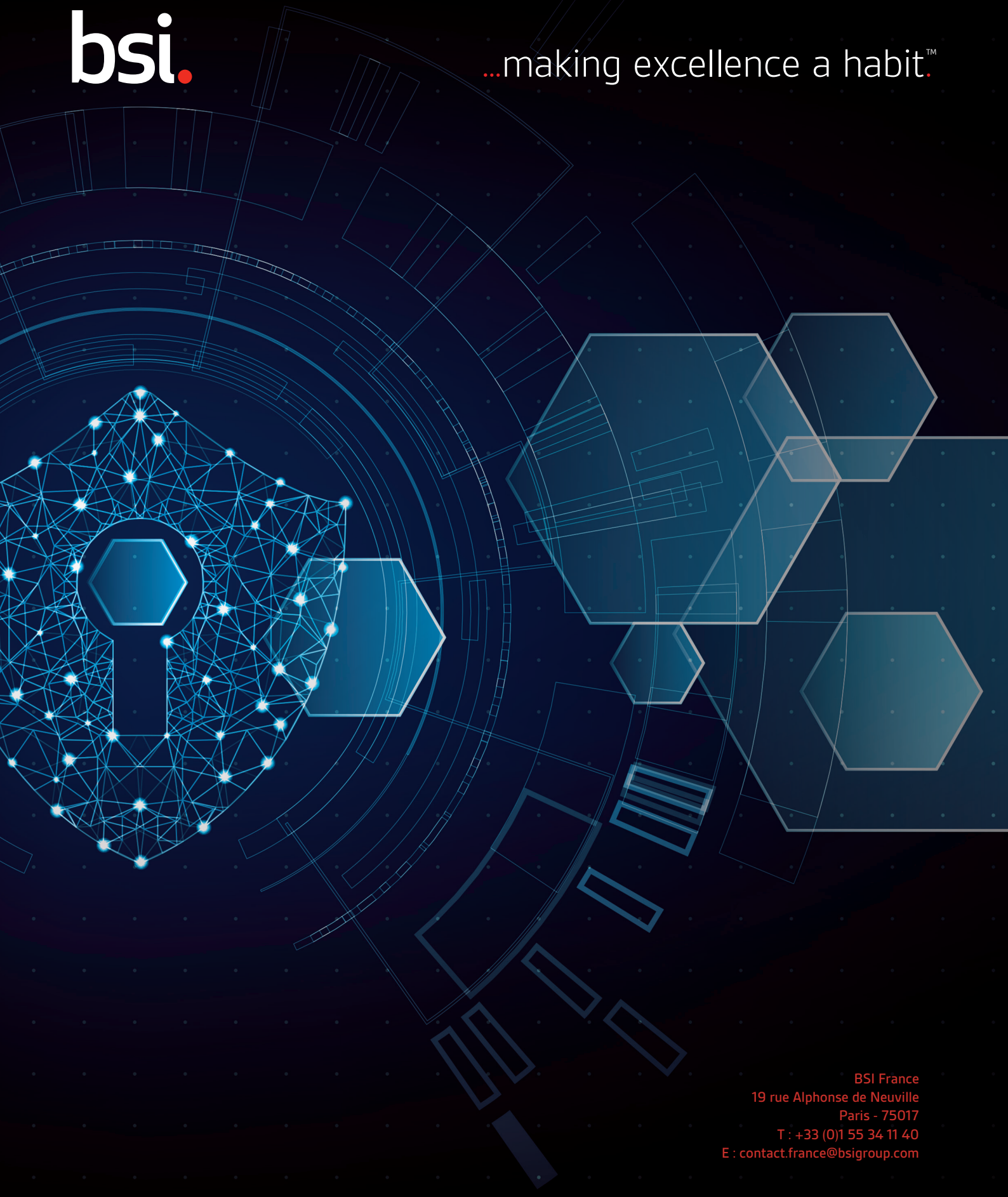
## 3 Obtenir la certification

La certification BSI envoie un signal fort à vos clients, concurrents, fournisseurs, employés et investisseurs, attestant de votre volonté d'atténuer les risques liés à la cybersécurité et de poursuivre dans cette voie. La certification est un élément important pour toutes les entreprises, petites et grandes. Par ailleurs, les experts BSI ne se contentent pas d'évaluer votre conformité aux normes, ils vous soutiennent à toutes les étapes dans votre politique d'amélioration continue.

bsi.

bsi.

...making excellence a habit.™



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