Faire face aux menaces cyber

20 septembre 2016

Rapport du Lloyd's

LLOYD'S

Sommaire

Section 1
Synthèse

1.1 Synthèse

Aujourd'hui, presque toutes les entreprises, indépendamment de leur taille ou de leur situation géographique, dépendent des technologies numériques. Ces dernières leur permettent d'être plus efficaces, de réduire leurs coûts et de s'ouvrir à de nouveaux marchés, mais d'un autre côté, elles les rendent plus vulnérables face aux attaques cyber. Au cours des deux dernières années, un certain nombre d'événements cyber très médiatisés, notamment en matière d'atteinte à la protection des données impliquant des fuites d'informations clients, ont placé la sécurité informatique sur le devant de la scène.

En 2018, l'Union Européenne introduira le règlement général sur la protection des données (GDPR en anglais), renforçant encore davantage le caractère urgent de cette question. Ce règlement vise à définir des règles strictes pour toutes les entreprises qui traitent des données appartenant aux consommateurs européens.

Le Lloyd's, à la pointe de l'assurance cyber au niveau mondial, a commandé cette étude pour comprendre les mesures de sécurité mises en place par les entreprises européennes et comment ces dernières se préparent à l'entrée en vigueur du GDPR.

L'étude a permis d'interroger 346 dirigeants de grandes entreprises ayant un chiffre d'affaires supérieur ou égal à 250 millions d'euros dans toute l'Europe. Les postes occupés par les personnes interrogées étaient les suivants : président-directeur général (PDG) ; directeur financier ; directeur opérationnel ; directeur des systèmes d'information (DSI) ; directeur des techniques informatiques (DTI) ; directeur des risques ; et conseiller juridique.

La plupart des grandes entreprises européennes a été victime d'une atteinte à la protection des données au cours des cinq dernières années mais ne s'inquiète pas de l'éventuelle récurrence d'un tel incident.

- 92 % des personnes interrogées déclarent que leur entreprise a été victime d'une fuite de données au cours des cinq dernières années, mais seulement 42 % s'inquiètent du fait qu'elles pourraient souffrir d'une nouvelle intrusion à l'avenir.

L'intérêt pour les questions liées aux menaces cyber n'a cessé de croître dans les conseils d'administration tout au long de l'année passée au point que c'est désormais le directeur général, et non pas le directeur des systèmes d'information, qui définit la stratégie en matière de sécurité informatique.

- Les plans de protection contre les fuites de données sont maintenant gérés en majorité par les directeurs généraux (dans 54 % des cas) selon les propos recueillis. A contrario, les directeurs des systèmes d'information mènent les prises de décisions dans seulement 10 % des entreprises. Ce phénomène fait écho à un certain nombre d'incidents cyber dans les entreprises du monde entier qui, bien souvent, ont eu un impact significatif sur les résultats ou le cours des actions, et, dans certains cas, ont pu causer le départ forcé des membres de la direction.

Globalement, les personnes interrogées sont conscientes de l'existence du règlement général sur la protection des données de l'UE, mais n'en comprennent souvent pas l'enjeu, ce qui pourrait s'avérer dangereux.

- 97 % des personnes interrogées ont entendu parler du GDPR mais seulement 7 % d'entre elles affirment bien le connaître ; 57 % déclarent qu'elles ne savent rien ou très peu de choses sur cette nouvelle règlementation, malgré les répercussions financières et juridiques sérieuses en cas de non-respect des règles.

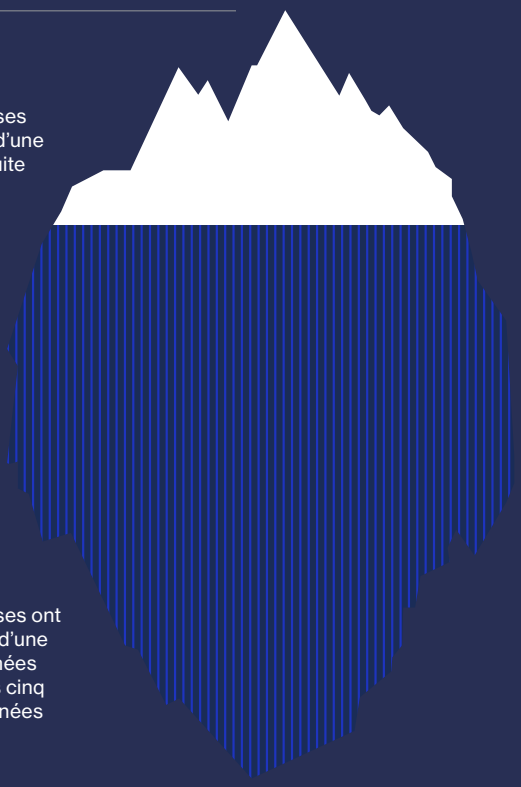
- Plus de la moitié des entreprises interrogées ont conscience que le GDPR pourrait entraîner plus de contrôles règlementaires (64 %), des sanctions financières (58 %), une baisse du cours des actions (57 %) et une atteinte à la réputation (52 %), mais seulement 13 % pensent qu'elles pourraient perdre des clients.

1.2 Conclusion

Les entreprises européennes doivent faire face à un risque cyber en constante évolution. L'introduction du GDPR attirera l'attention sur la sécurisation des données dans leurs opérations. En effet, les organismes de contrôle, les actionnaires et les clients s'en serviront pour tenir les entreprises responsables de l'élévation des standards en matière de sécurité informatique. En travaillant en partenariat avec des experts, tels des avocats, des assureurs et des experts de la sécurité informatique, les entreprises seront mieux à même de comprendre les risques qui les guettent et tenter de les réduire afin de protéger leurs bilans.

42%

des entreprises s'inquiètent d'une potentielle fuite de données



92%

des entreprises ont été victimes d'une fuite de données au cours des cinq dernières années

Le rôle de l'assurance cyber

- Selon cette étude, 73% des dirigeants d'entreprise n'ont qu'une connaissance limitée de l'assurance cyber et 50% d'entre eux ne savent pas que des garanties risques cyber existent en cas de fuites de données.
- Les produits d'assurance cyber garantissent non seulement les versements de fonds après une attaque cyber mais donnent aussi accès à des conseils d'experts afin d'améliorer la sécurité et l'aide sur site pendant la période de crise.
- Collaborer avec des assureurs qui comprennent bien ce type de risque dans sa globalité est bénéfique à l'entreprise lorsqu'elle assure sa sécurité. Les assureurs peuvent aider les entreprises à identifier les risques et les failles et peuvent donc dès le départ réduire le risque d'atteinte à la protection des données.
- Tous ces éléments peuvent aider à protéger les bilans de l'entreprise mais aussi à élever les standards en matière de sécurité informatique et de réduire les risques potentiels dans tout un secteur.

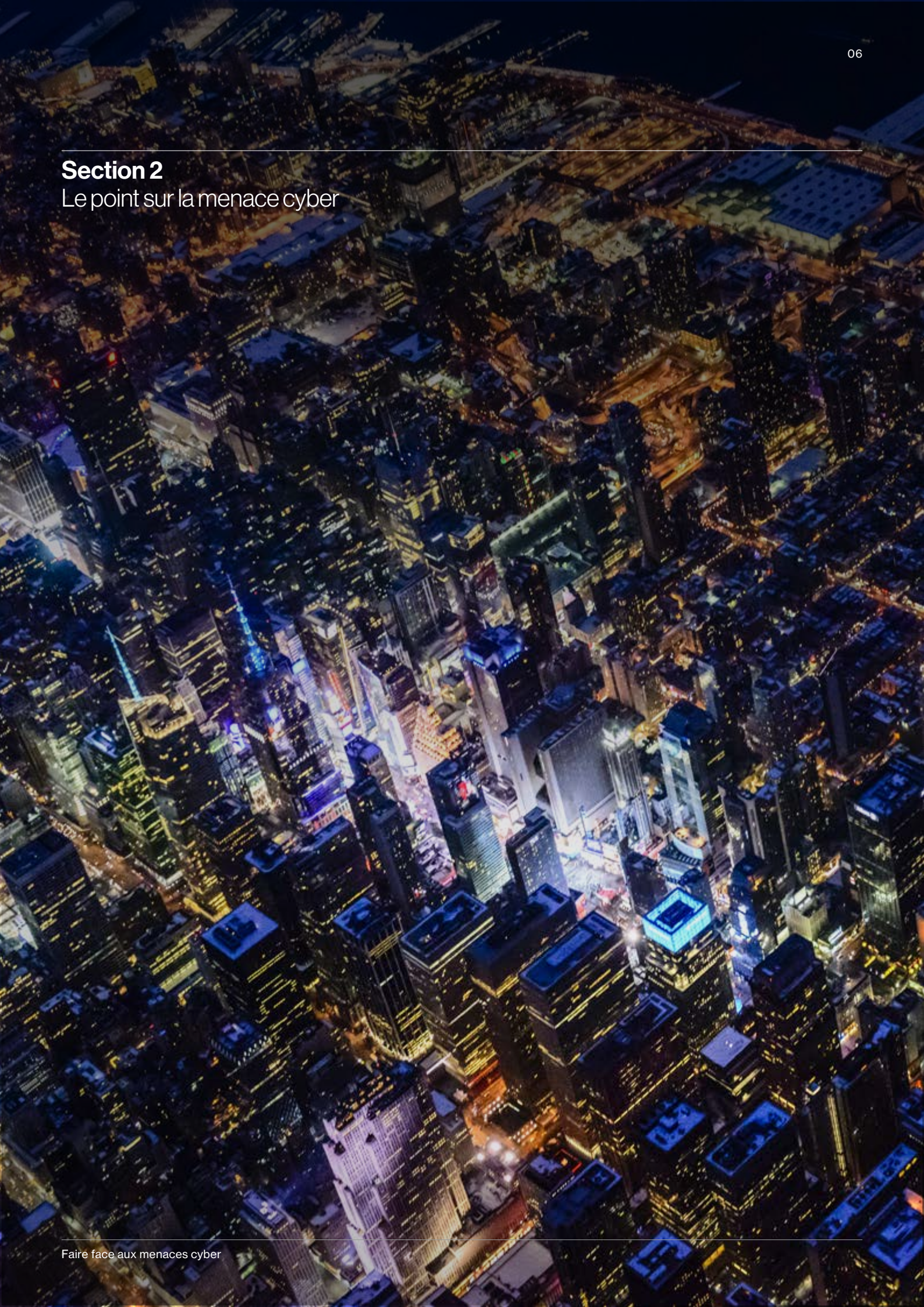
Rendez-vous sur www.lloyds.com/cyber

97%

des entreprises ont entendu parler du GDPR, le nouveau règlement de l'UE

57%

des entreprises ne connaissent pas ou ne connaissent que très peu le GDPR, le nouveau règlement de l'UE



Section 2
Le point sur la menace cyber

2.1 La montée en puissance de la menace cyber

Aujourd'hui, presque toutes les entreprises, indépendamment de leur taille ou de leur situation géographique, dépendent des technologies numériques. Les grandes enseignes, les sociétés de services financiers, les marques de distribution font toutes appel à la technologie numérique pour mener leurs activités, surveiller leurs stocks, concevoir leurs produits, communiquer et stocker leurs données clients.

Mais alors que ces technologies leur permettent d'être plus efficaces, de réduire leurs coûts et de s'ouvrir à de nouveaux marchés, elles les rendent aussi plus vulnérables aux attaques cyber.

C'est pour cette raison que la sécurité informatique est devenue un enjeu majeur pour les entreprises. Le domaine cyber est désormais une menace qui, au même titre que des risques bien connus comme les dommages aux biens, le terrorisme et les catastrophes naturelles, doit être évaluée, atténuée et gérée par les entreprises.

La prise de conscience de l'existence du risque cyber au sein des entreprises a été provoquée par divers incidents très médiatisés qui se sont produits dans le monde ces dernières années. L'attaque cyber de grande envergure la plus récente au Royaume-Uni a été celle menée contre la société de télécoms TalkTalk à l'automne 2015. Ailleurs en Europe, diverses attaques ont tour à tour touché, entre autres, la chaîne de télévision française TV5 Monde, le système de contrôle du trafic aérien suisse, des entreprises du secteur pétrolier et de l'énergie en Norvège et un sidérurgiste allemand. Aux États-Unis, plusieurs incidents informatiques ont fait la une des journaux depuis 2014, dont les attaques contre Sony, Target, Home Depot et Experian.

Parallèlement, le marché du Lloyd's, qui a lancé la toute première police d'assurance cyber il y a 10 ans, a vu le marché de l'assurance cyber croître rapidement. Il existe maintenant 65 assureurs qui proposent une assurance cyber sur le marché du Lloyds, pour une capacité combinée de 300 millions de livres sterling. Leur activité représente un quart du marché de l'assurance cyber dans le monde, faisant ainsi du Lloyd's le centre névralgique mondial de l'assurance cyber.

Ce rapport, basé sur une étude menée auprès de 346 décisionnaires de grandes entreprises en Europe, analyse la façon dont les dirigeants abordent le problème de la sécurité informatique et les mesures qu'ils mettent en place pour s'assurer que leur entreprise est correctement préparée à une attaque cyber.

Le rapport enquête également sur la façon dont se sont préparées les entreprises européennes aux nouvelles règles européennes édictées par le règlement général sur la protection des données (GDPR) de l'UE, prévue en 2018. Ce nouveau règlement durcira considérablement les règles, aggravera les responsabilités déjà existantes en la matière, et imposera aux entreprises de traiter et conserver les données de manière plus stricte. Il prévoit aussi un certain nombre de mesures dans le cas où une entreprise serait victime d'une atteinte à la protection de ses données, dont l'obligation pour elle de signaler toute attaque cyber dans les 72 heures, sous peine d'amendes importantes.

Ce rapport aborde un type d'incident cyber, qui est la violation des données, ceci parce que la protection des données confidentielles, en particulier les informations financières ou les données sur la santé des personnes, est considérée comme une priorité par la plupart des entreprises. Ces données représentent leur principal actif numérique et de ce fait, sont la cible de la plupart des attaques cyber.

2.2 Les fuites de données

Quel enjeu représente la fuite de données pour les entreprises européennes à l'heure actuelle ? Pour mesurer l'ampleur du phénomène, les personnes interrogées ont dû préciser si leur entreprise avait déjà été victime d'une fuite de données.

92 % des personnes interrogées ont déclaré que leur entreprise avait été victime d'une fuite de données au cours des cinq dernières années, tandis que 3 % ont déclaré y avoir échappé de peu. Seulement 5 % des personnes interrogées n'avaient pas subi de fuite de données ou ne pensaient pas en avoir subi.

Parmi les affirmations suivantes, laquelle se rapproche le plus de l'expérience de votre entreprise en matière de fuite de données, au cours des cinq dernières années ?

Base : Total des personnes interrogées (346) : Royaume-Uni (100) France (31) Allemagne (34) Italie (30) Espagne (30) Pays-Bas (31) Norvège (30) Danemark (30)

2.3 Menaces internes et externes

Les fuites de données peuvent être provoquées par différents types d'attaques cyber, certaines très sophistiquées et malveillantes, d'autres accidentelles ou relativement peu préjudiciables. L'étude a cherché à identifier les menaces qui inquiétaient le plus les entreprises.

Les menaces cyber étaient divisées en deux catégories, « internes » et « externes ». Les menaces internes sont typiquement celles qui émanent de l'entreprise elle-même, soit à cause d'une erreur humaine, en raison d'informations ou d'équipements volés ou perdus, soit à cause d'un employé malveillant divulguant intentionnellement des informations confidentielles. Les menaces externes font plutôt appel à des techniques plus sophistiquées comme le hacking, le phishing, les rançongiciels et les logiciels malveillants (voir glossaire ci-dessous).

L'étude a montré que les menaces externes inquiétaient davantage les entreprises que les menaces internes. Les menaces internes les plus redoutées par les entreprises proviennent d'outils à faible niveau de technicité, 42 % des personnes interrogées citant la perte physique de documents papiers comme étant une préoccupation majeure. Le même pourcentage considère aussi la divulgation intentionnelle d'informations par un employé comme une menace importante.

La menace externe citée en premier est l'intrusion dans le système informatique, ou « hacking ». La moitié (51%) des entreprises interrogées affirment que le risque d'être victime d'un hacking à des fins financières les inquiète, tandis que 46 % de ces mêmes entreprises craignent d'être victime d'un hacking pour des raisons politiques. 41% considèrent l'intrusion d'un concurrent dans le système informatique comme une menace sérieuse.

Il n'est pas surprenant que le hacking se classe en haut du tableau étant donné les violations de données majeures qui ont eu lieu récemment. Les sociétés TalkTalk, Sony et Home Depot, pour n'en nommer que trois, ont toutes été victimes d'une attaque cyber récemment. Bien que les motivations profondes de ces incidents soient souvent obscures, des attaques de ce type sont souvent menées pour vendre au plus offrant des informations clients.

Parfois, ces attaques sont lancées à des fins politiques, en particulier contre des entreprises qui opèrent dans des domaines sensibles d'un point de vue géopolitique, comme l'énergie ou les ressources naturelles. Nous voyons de plus en plus d'organisations être attaquées par des groupes de hackers malveillants, aux motivations politiques clairement définies. Si l'étendue réelle de la menace d'espionnage industriel peut être difficile à mesurer avec précision, les dirigeants la mettent en troisième position de leurs préoccupations, ce qui montre la gravité pour eux de l'intrusion de la concurrence dans leurs systèmes de données.

Glossaire sur la menace cyber

- Hacking : recherche et exploitation des failles dans un système ou réseau informatique, souvent afin d'obtenir un gain financier
- Phishing : tentative d'obtenir des informations sensibles en se faisant passer pour une personne ou une entreprise de confiance dans un e-mail
- Fraude au président : attaque de type phishing qui consiste à se faire passer pour un directeur, souvent le PDG d'une entreprise
- Malware : (fusion des mots anglais « malicious » et « software », c'est-à-dire « logiciel malveillant ») tout logiciel utilisé pour interrompre des opérations informatiques, recueillir des informations sensibles ou accéder à des systèmes informatiques privés
- Ransomware (ou rançongiciel) : type de logiciel qui affecte un ordinateur et demande le paiement d'une rançon pour le faire fonctionner à nouveau correctement

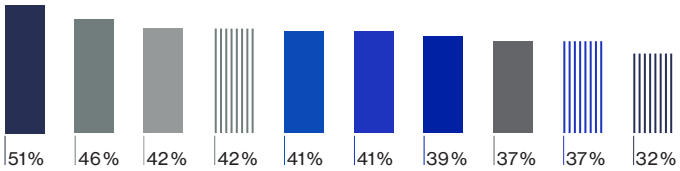
51 %

craignent d'être victime d'un hacking mené afin d'obtenir un gain financier

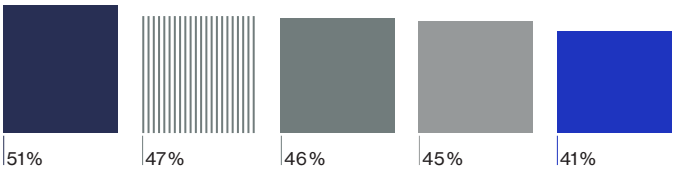
2.3 Menaces internes et externes

- Piratage informatique («hacking») – gain financier
- Piratage informatique («hacking») – concurrent
- Piratage informatique («hacking») – motivations politiques
- Erreur humaine/divulgation involontaire
- Phishing
- Équipements perdus, jetés ou volés
- Rançongiciel («ransomware»)
- Logiciel malveillant
- Perte physique de documents papier ou de matériel non électronique
- Collaborateur divulguant intentionnellement des informations

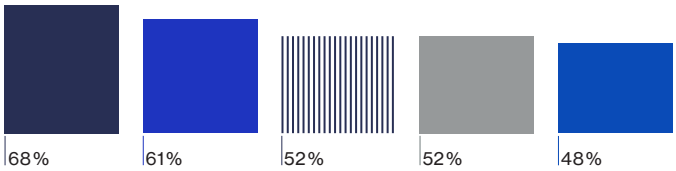
Total



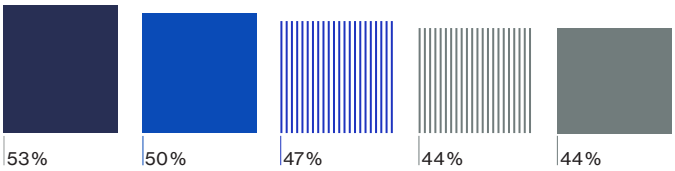
Royaume-Uni



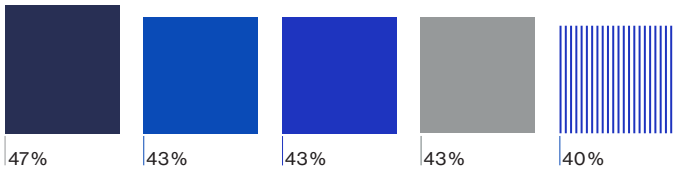
France



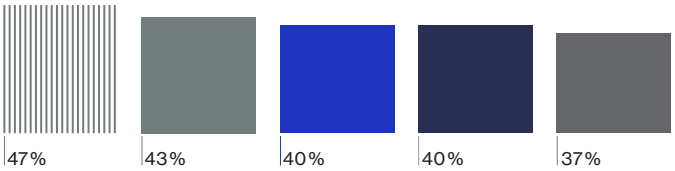
Allemagne



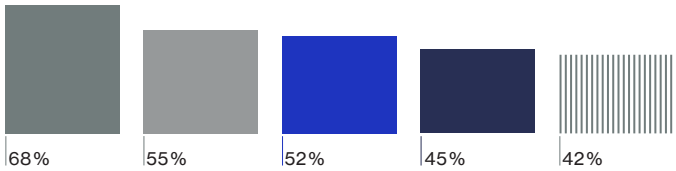
Italie



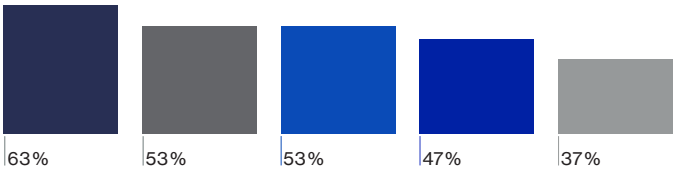
Espagne



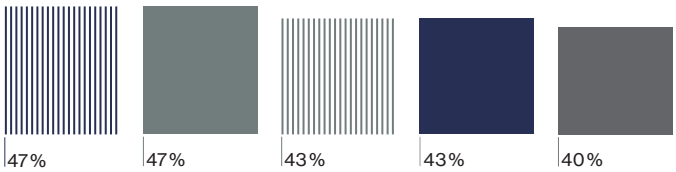
Pays-Bas



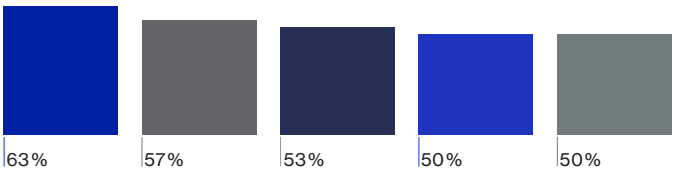
Norvège



Suède



Danemark



Base: Total des personnes interrogées (346): Royaume-Uni (100) France (31) Allemagne (34) Italie (30) Espagne (30) Pays-Bas (31) Norvège (30) Danemark (30)

2.4 Une fausse impression de sécurité informatique

Bien que 92 % des entreprises aient été victimes d'une fuite de données au cours des cinq dernières années, seuls 42 % des personnes interrogées s'inquiètent du fait qu'elles pourraient souffrir d'une nouvelle intrusion à l'avenir.

92 %

des entreprises ont été victimes d'une fuite de données

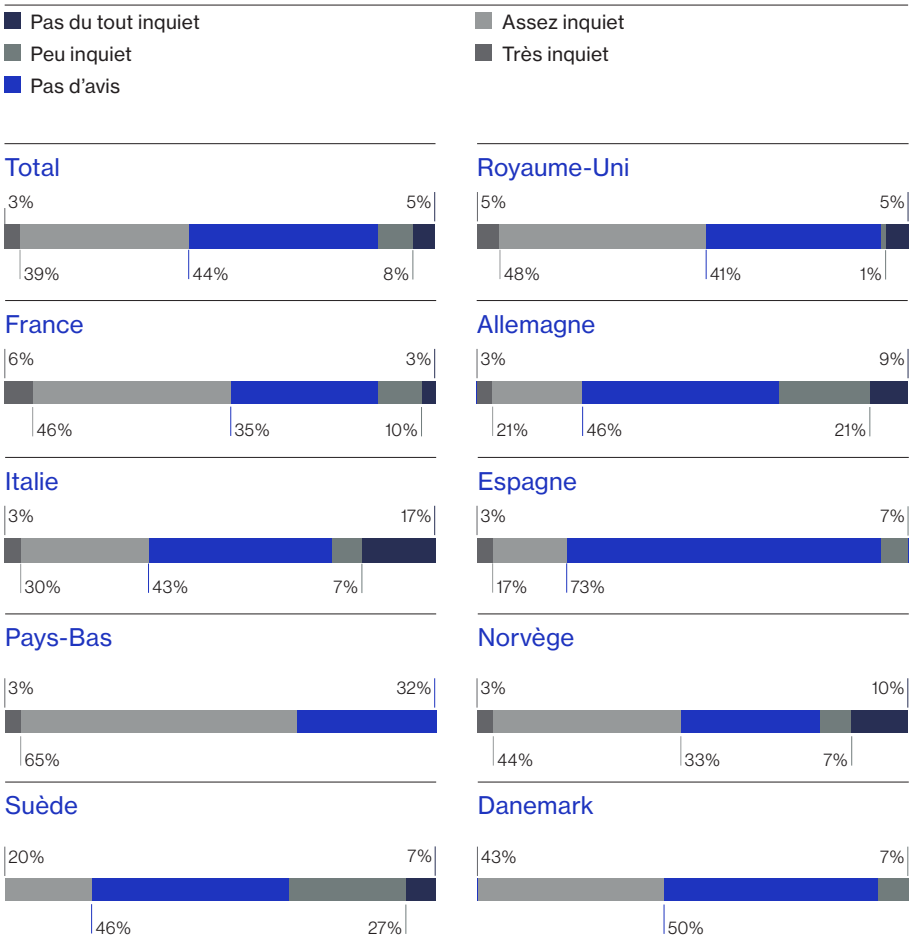
42 %

des entreprises s'inquiètent d'une potentielle fuite de données

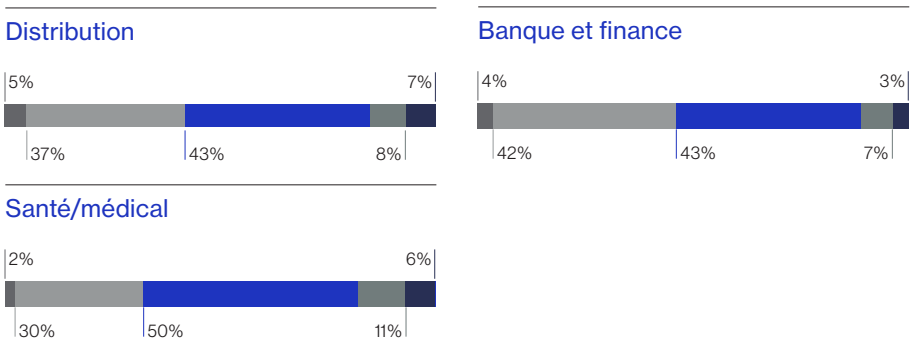
Les résultats diffèrent légèrement d'un secteur à l'autre. Ce sont les sociétés du secteur financier qui s'inquiètent le plus d'une fuite de données (46 %), ce qui est compréhensible étant donné le nombre d'informations sensibles qu'elles détiennent sur leurs clients. Les entreprises du secteur de la santé sont celles qui s'en inquiètent le moins (32 %), ce qui peut paraître surprenant car la valeur des dossiers médicaux est de plus en plus grande et de ce fait, ces derniers sont désormais particulièrement recherchés par les hackers.

Ces résultats montrent soit que les entreprises font confiance aux mesures de sécurité informatique qu'elles ont mises en place, soit qu'elles se satisfont de leur résilience aux attaques cyber. Quelle que soit la réponse, le fait est que la technologie qui permet de mettre en œuvre une attaque cyber évolue constamment, empêchant ainsi les entreprises de se protéger à 100 %. Tant que les entreprises ne prendront pas la sécurité informatique vraiment au sérieux, elles resteront vulnérables à de futures attaques cyber.

Considérant l'entreprise dans laquelle vous travaillez, sur une échelle de 1 à 5 où 1 signifie « pas du tout inquiet » et 5 « très inquiet », dans quelle mesure êtes-vous inquiet de la survenue d'une fuite de données dans votre entreprise ?



Base: Total des personnes interrogées (346) : Royaume-Uni (100) France (31) Allemagne (34) Italie (30) Espagne (30) Pays-Bas (31) Norvège (30) Danemark (30)



Base: Total des personnes interrogées (346) : Distribution (109) Banque et finance (95) Santé/médical (90)

Section 3
Préparation et riposte

3.1 Carence dans la préparation...

Comme nous l'avons vu dans la section précédente, 92 % des entreprises ont été victimes d'une fuite de données au cours des cinq dernières années. Les personnes interrogées devaient évaluer dans quelle mesure elles se sentaient prêtes à gérer la survenance de ce type d'incident. Les entreprises ont dû estimer leur niveau de préparation à une fuite de données sur la base de trois critères :

1. Mise en place d'une cellule de crise et interventions immédiates : p. ex. communiquer la nouvelle aux clients et mettre à jour les systèmes informatiques.
2. Limitation des atteintes à la réputation, p. ex. par le biais des relations publiques, de la publicité et d'autres activités de communication.
3. Implications règlementaires : p. ex. coopération avec les enquêteurs ou adaptation à un changement de règlementation.

93 %

des entreprises se disent « prêtes » ou « bien préparées » à intervenir en cas de crise

89 %

se disent « prêtes » ou « bien préparées » à agir en cas d'atteinte à la réputation

87 %

prennent en compte les implications règlementaires

La plupart des entreprises dispose de processus et de procédures à mettre en place en cas d'incident cyber, mais cela ne veut pas dire que ces entreprises soient bien préparées à un tel incident. Beaucoup d'entreprises se concentrent sur l'élaboration d'un plan d'intervention qui définit ce qu'il convient de faire en cas de fuite de données, mais il existe pourtant toute une série de mesures, couvrant l'incident en amont et en aval, qui doivent être appliquées si une entreprise veut se préparer convenablement.

Les entreprises doivent s'assurer que leurs systèmes sont correctement testés et validés en externe avant de pouvoir être certaines de leur niveau de préparation. Même si ces actions ont été menées à bien, il est crucial d'être constamment vigilant et de mettre régulièrement à jour les plans d'intervention à mesure qu'émergent de nouvelles menaces.

3.2 Qui est responsable?

La sécurité a, pendant longtemps, relevé uniquement de la compétence du service informatique. Aujourd'hui, l'importance de la sécurité des données est telle qu'elle occupe une place de choix dans la liste des priorités des dirigeants.

Ce changement a eu lieu de manière remarquablement rapide. Une enquête du groupe Marsh datant de l'année dernière [2015] montre que seulement 17% des entreprises européennes citaient le risque cyber parmi les cinq principaux risques pour leur entreprise, tandis que 25% ne mentionnaient pas du tout ce risque. Presque les deux tiers des entreprises (65%) considéraient que les services informatiques étaient les principaux responsables de la gestion de la menace cyber au sein de leur entreprise et 11% estimaient que c'était au conseil d'administration d'en prendre la responsabilité.

L'étude du Lloyd's, menée 9 mois plus tard, conclut que les conseils d'administration en Europe adoptent désormais une approche plus pragmatique afin de mieux appréhender la menace cyber.

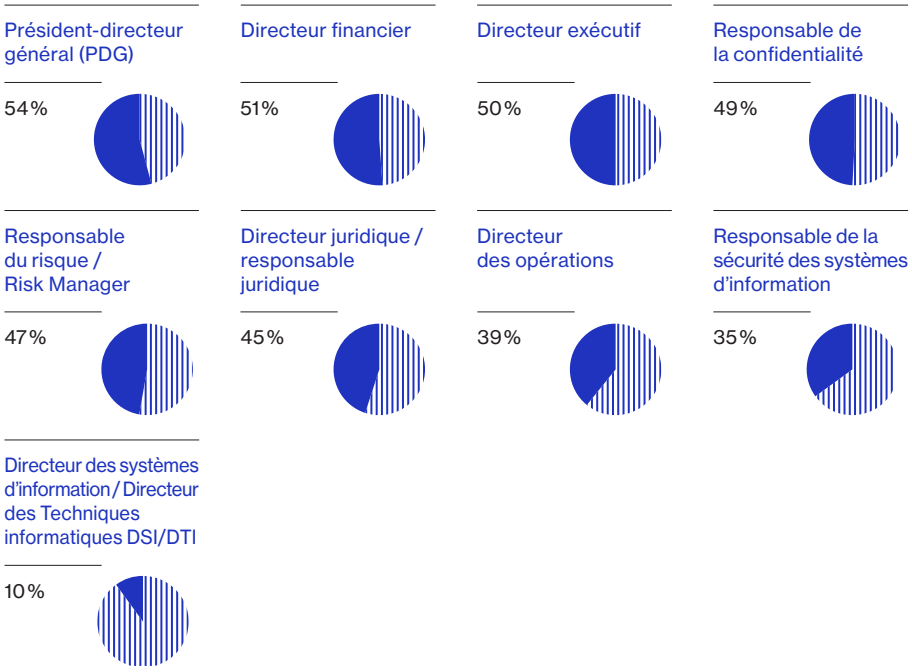
Les personnes interrogées ont dû indiquer quelle était la personne, au sein de leur entreprise, la plus à même de prendre des décisions en matière de politique de sécurité informatique en cas de violation de données. La majorité d'entre elles (54%) a désigné le PDG. Les cas où ce sont les cadres qui traitent la question de la menace cyber au quotidien sont minoritaires: 35% des personnes interrogées désignent le responsable de la sécurité informatique comme responsable dans leur entreprise et seulement 10% désignent le directeur informatique ou le directeur des techniques informatiques comme responsable. Dans 96% des cas, un membre de la direction est désigné comme étant la force d'impulsion.

Il est probable que la série récente de fuites de données et leurs conséquences (chute du cours des actions, coûts, procès), très médiatisées, a eu pour effet de convaincre les dirigeants de mettre en place des stratégies de sécurité informatique ambitieuses. Les actionnaires attendent des dirigeants d'entreprise qu'ils assument la responsabilité de la sécurité informatique et qu'ils entreprennent tout ce qui est en leur pouvoir pour limiter les risques, qui affectent à terme les résultats financiers de l'entreprise.

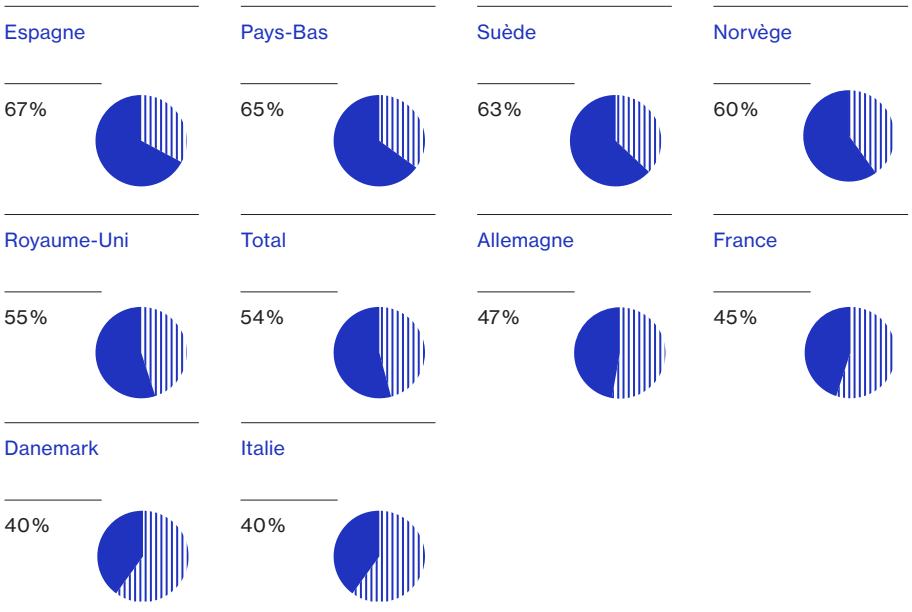
Les dirigeants ont de bonnes raisons de prendre cette question très au sérieux car la pérennité de leur travail est directement liée aux conséquences d'une faille de sécurité. Le PDG de la chaîne de supermarchés américaine Target et celui de l'entreprise aérospatiale autrichienne FACC ont tous deux perdu leur emploi pour des raisons liées à un incident cyber.

Il est encourageant, ainsi que le montre cette étude, de constater que les dirigeants sont de plus en plus nombreux à prendre la menace cyber au sérieux. Les changements à venir dans la règlementation de l'UE devraient pousser toutes les entreprises en Europe à prendre davantage en compte cette menace.

Qui dans votre entreprise prend les décisions concernant la protection et la planification des actions en cas de violation de données?



Président-directeur général (PDG)



Base: Total des personnes interrogées (346)

Section 4
Comprendre le GDPR

4.1 Une nouvelle ère de réglementation informatique

L'introduction du règlement général sur la protection des données (GDPR) en 2018 va bouleverser la règlementation informatique en Europe. Le nouveau règlement aura également des répercussions dans le reste du monde, répercussions qui ne sont pas encore bien comprises par les entreprises elles-mêmes.

Le GDPR consacre le droit fondamental à la protection de la vie privée du consommateur, tel que le « droit à l'oubli » et le droit de s'opposer à des activités de profilage, que les entreprises seront tenues de respecter.

Il est important de souligner que le GDPR ne s'appliquera pas uniquement aux entreprises des États membres de l'UE. Toute entreprise qui propose des biens et des services à des citoyens de l'UE, ou qui suit leur comportement, devra également se conformer à ces nouvelles règles. Cela signifie que de nombreuses entreprises aux États-Unis et en Asie, par exemple, seront concernées par la portée juridictionnelle du GDPR.

Le GDPR ne peut donc pas être ignoré. Cette enquête porte sur le degré de préparation des entreprises au GDPR, dont l'entrée en vigueur aura lieu dans moins de deux ans.

Qu'est-ce que le GDPR?

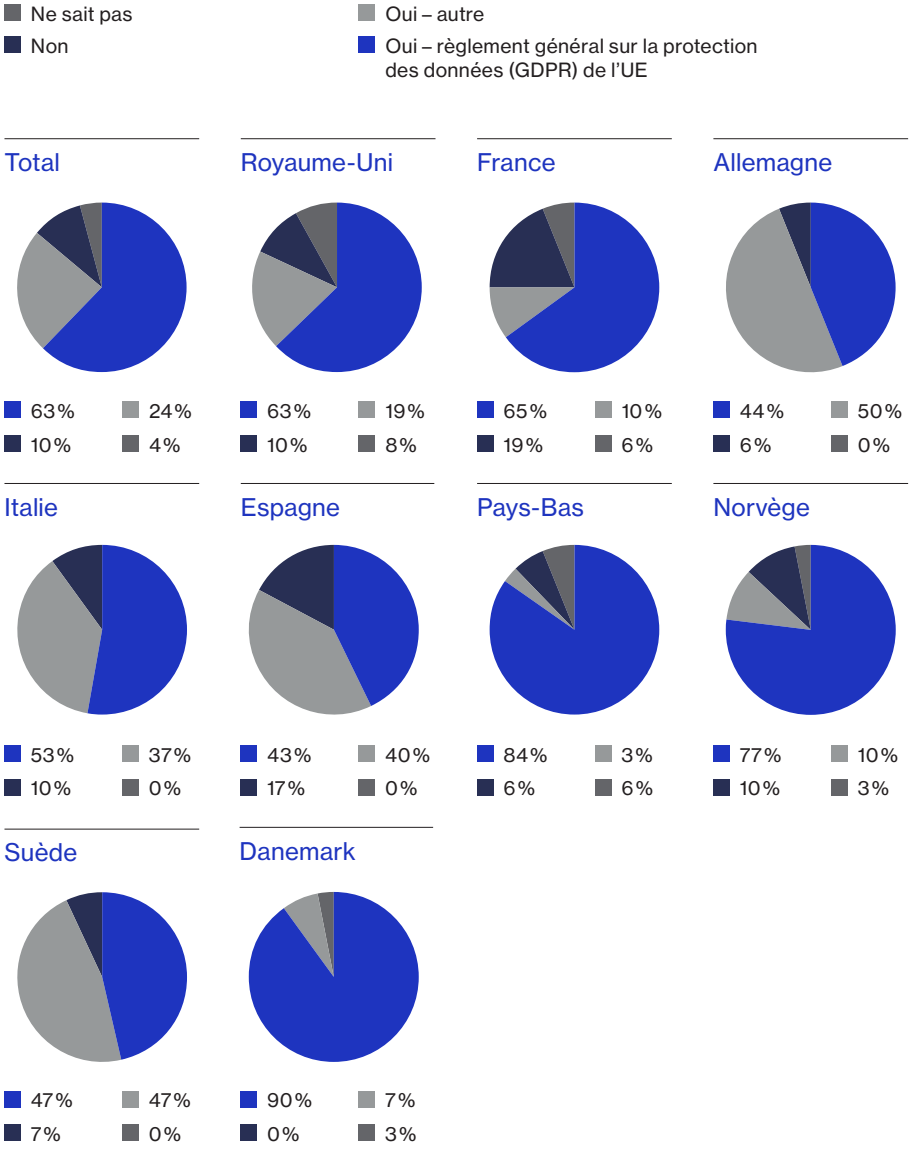
- Le règlement général sur la protection des données (GDPR) est une nouvelle législation européenne qui vise à harmoniser les diverses lois sur la protection des données existant au sein de l'UE et à adapter la législation européenne à l'ère du Big data.
- Il exige notamment des entreprises qu'elles rapportent toute violation de données à l'organisme de contrôle compétent dans les 72 heures ainsi qu'aux personnes impactées sans délai injustifié.
- Les sanctions prévues incluent des amendes pouvant se chiffrer jusqu'à 4 % du chiffre d'affaires annuel mondial ou à 20 millions d'euros, la somme la plus forte étant retenue, pour les entreprises qui subissent des fuites de données. Les personnes impactées pourront aussi demander réparation aux organisations en cas de pertes financières ou de préjudice moral.
- Le règlement entrera en vigueur le 25 mai 2018 dans tous les États membres de l'UE, et affectera toute entreprise menant des activités touchant des citoyens de l'UE, indépendamment de sa localisation.

4.2 Prise de conscience et compréhension

Étant donné l'importance du GDPR, qui a été annoncé dès 2012 et dont l'entrée en vigueur est imminente, les entreprises auraient déjà pu prendre des mesures d'envergure. Or, l'étude révèle une réalité plus contrastée.

Elle montre que la majorité des entreprises connaît le GDPR. Lorsqu'on leur demande si elles connaissent de nouvelles règlementations qui pourraient affecter le domaine de la protection des données, 63% des personnes interrogées mentionnent le GDPR. 24% font référence à d'autres règlementations, qui pourraient concerner pour certaines des évolutions au niveau national en matière de protection des données.

Connaissez-vous les nouvelles règlementations ou les changements de règlementations liés à la protection des données ?



Base: Total des personnes interrogées (346): Royaume-Uni (100) France (31) Allemagne (34) Italie (30) Espagne (30) Pays-Bas (31) Norvège (30) Danemark (30)

4.2 Prise de conscience et compréhension

Lorsque le GDPR est évoqué auprès des entreprises, 97% d'entre elles affirment le connaître. Cependant, ce chiffre cache un manque de compréhension dudit règlement. Seulement 7% des personnes interrogées affirment «très bien» connaître le GDPR, tandis que plus de la moitié (57%) admettent le connaître «peu» ou «pas du tout». Vu l'importance du GDPR pour les entreprises, ce manque de connaissance est surprenant.

97%

des personnes interrogées ont entendu parler du GDPR

57%

admettent connaître «peu» ou «pas du tout» le GDPR

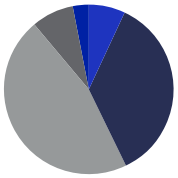
Le GDPR prévoit par exemple des sanctions financières importantes à l'encontre des entreprises qui ne se conformeraient pas à la nouvelle règlementation (jusqu'à 4% de leur chiffre d'affaires mondial). Il définit également de nouveaux standards pour plus de transparence sur l'utilisation des données clients, plus de sécurité pour les systèmes qui contiennent ces données et pour plus de rapidité sur l'information des clients en cas de fuite de données. Aucune de ces obligations ne sera facile à respecter, elles demanderont du temps, des investissements et des efforts.

Les résultats suggèrent que les entreprises doivent faire plus d'efforts pour comprendre en quoi les règles du GDPR affecteront leur organisation et quelles sont leurs responsabilités.

Dans quelle mesure connaissez-vous le règlement général sur la protection des données (GDPR) de l'UE?

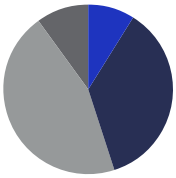
- Je connais très bien le GDPR de l'UE
- J'ai entendu parler du GDPR de l'UE mais je n'en connais pas tous les détails
- Je n'ai pas entendu parler du GDPR de l'UE et je n'en connais rien
- Je connais assez bien le GDPR de l'UE
- J'ai entendu parler du GDPR de l'UE mais je n'en connais pas du tout les détails

Total



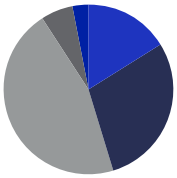
7% 36% 46% 8% 3%

Royaume-Uni



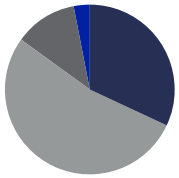
9% 36% 45% 10% 0%

France



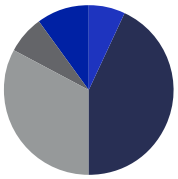
16% 29% 45% 6% 3%

Allemagne



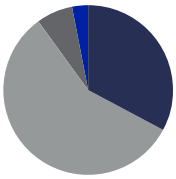
0% 32% 53% 12% 3%

Italie



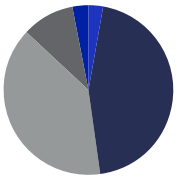
7% 43% 33% 7% 10%

Espagne



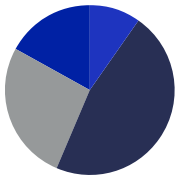
0% 33% 57% 7% 3%

Pays-Bas



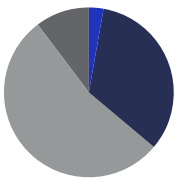
3% 45% 39% 10% 3%

Norvège



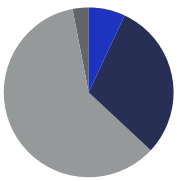
10% 47% 27% 0% 17%

Suède



3% 33% 53% 10% 0%

Danemark



7% 30% 60% 3% 0%

Base: Total des personnes interrogées (346): Royaume-Uni (100) France (31) Allemagne (34) Italie (30) Espagne (30) Pays-Bas (31) Norvège (30) Danemark (30)

4.3 Reconnaître les incidences pour les entreprises

Bien que la majorité des dirigeants et responsables admette ne pas bien connaître le GDPR, 66% d'entre eux affirment qu'ils comprennent les implications du GDPR en cas de fuite de données dans leur entreprise.

Les personnes interrogées sur ce sujet répondent se focaliser sur deux problématiques clés: l'impact financier et l'impact règlementaire. En tête de liste des problématiques clés figurent les enquêtes des autorités de contrôle, 64% des entreprises désignant ce risque comme le plus probable, viennent ensuite les sanctions financières ou amendes (58%) et l'impact sur les profits ou le cours des actions (57%) et seulement 13% des personnes interrogées s'inquiètent de la perte de clients.

64% enquête règlementaire

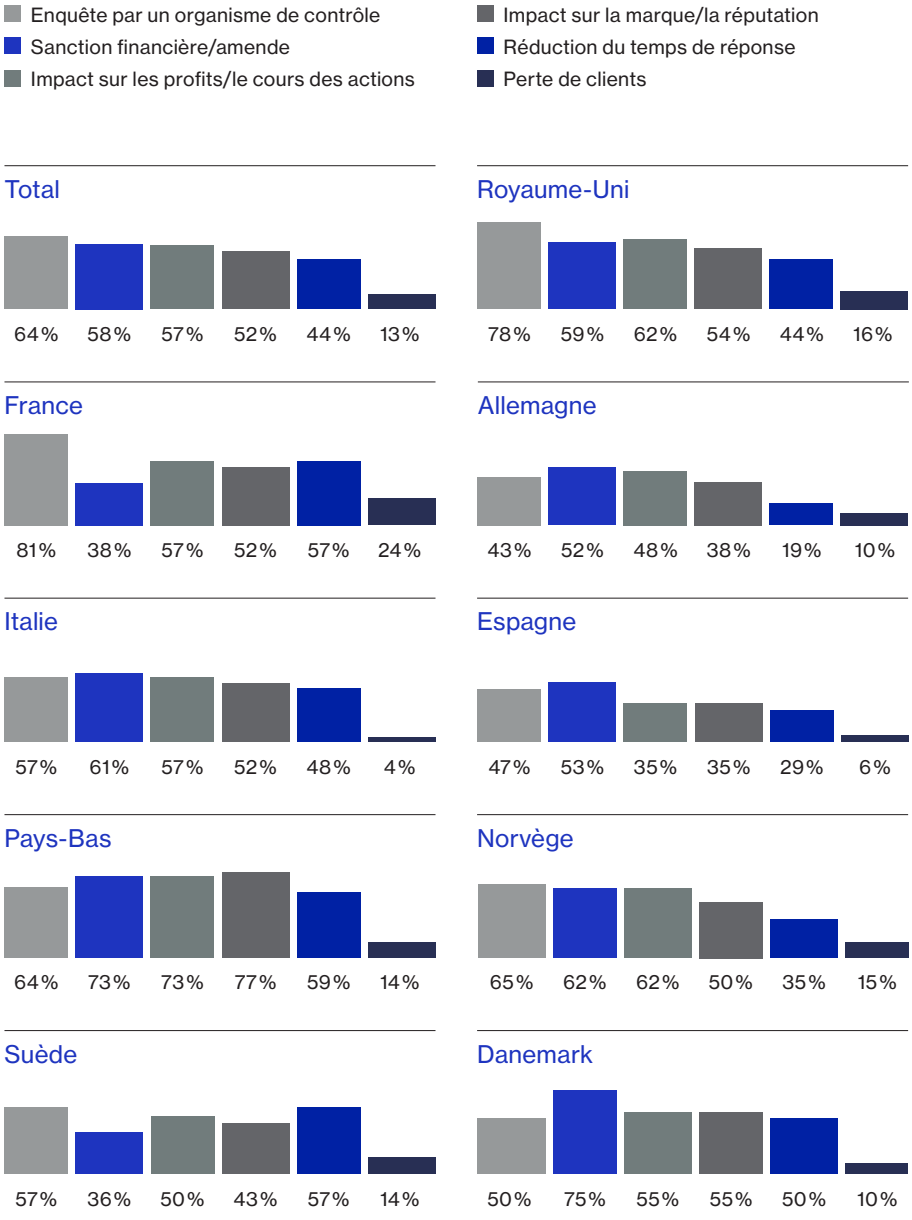
58% sanctions financières ou amendes

57% impact sur les profits/ le cours des actions

13% perte de clients

L'étude montre que la principale inquiétude des grandes entreprises européennes est l'incidence financière du GDPR en cas de fuite de données. L'attaque cyber contre TalkTalk, par exemple, a coûté à l'entreprise 60 millions de livres sterling et a entraîné une chute de 10% du cours de l'action le jour où l'événement a été annoncé. L'entrée en vigueur du GDPR risque d'augmenter encore l'impact financier d'une fuite de données.

En gardant à l'esprit les processus actuels de protection des données qui existent dans votre entreprise, quelles sont les incidences que le GDPR est susceptible d'avoir sur votre entreprise?



Base: Total des personnes interrogées (227): Royaume-Uni (63) France (21) Allemagne (21) Italie (23) Espagne (17) Pays-Bas (22) Norvège (26) Danemark (20)

Section 5
Conclusion

5.1 Conclusion

Le risque cyber est le risque le plus complexe, le plus récent et le plus critique pour votre entreprise à l'heure actuelle: la question est de savoir «quand» et non pas «si» une entreprise va être victime d'un piratage informatique.

Les incidents cyber peuvent provoquer l'interruption des activités d'une entreprise, entraîner des sanctions financières, accroître l'attention des organismes de contrôle et causer une atteinte à la réputation. Toutes ces menaces sur les profits, le cours des actions ou même la survie de l'entreprise ne sont pas à prendre à la légère. Dans ce contexte, il peut être difficile pour les dirigeants de savoir comment agir pour protéger leur entreprise.

Les résultats de cette étude montrent que bien que de nombreuses entreprises paraissent confiantes dans leur niveau de préparation au GDPR, leur compréhension de ses incidences est faible. Des exemples récents de fuites de données suggèrent que les entreprises ne sont pas aussi bien préparées aux attaques cyber qu'elles le pensent.

Il reste 18 mois avant l'entrée en vigueur du GDPR, les entreprises ont donc encore le temps de mettre en conformité leurs process et leurs méthodes avec les règles du GDPR. Entretemps, il est essentiel que les entreprises continuent à revoir leur stratégie face à la menace cyber et à leur compréhension de ce risque. Les menaces cyber ne sont pas près de disparaître et tendent à se complexifier dans le temps. Il est presque impossible de se protéger à 100 % contre les attaques cyber.

Voici trois mesures que les dirigeants peuvent prendre en considération pour protéger leur entreprise:

1 Identifier les risques spécifiques auxquels vous êtes confronté

Recensez les incidents cyber les plus susceptibles de survenir dans votre entreprise. Créez des plans spécifiques pour diminuer le risque de survenance de ces incidents. Quels sont les événements rares que vous n'aviez pas pris en considération? Vos plans d'intervention doivent être régulièrement testés et mis à jour. Demandez à des conseillers externes de les contrôler. Travaillez ensemble sur différents scenarii et simulations. Assurez-vous de vous préparer correctement à agir en amont d'une fuite de données et à intervenir après, au-delà de la simple communication avec les clients affectés.

2 Informer sur la menace cyber et la règlementation dans toute votre entreprise

L'erreur humaine est à l'origine de nombreux incidents cyber, de la divulgation accidentelle au phishing. La connaissance ou non de ces problèmes relève de la culture de l'entreprise et l'impulsion doit nécessairement venir de la direction. Faites en sorte que l'ensemble du personnel soit formé et sache, par exemple, ce qu'il doit faire pour se conformer aux règles du GDPR.

3 Ne jamais cesser de se former sur le sujet

Les technologies numériques sont en perpétuelle évolution, tout comme les menaces cyber. Mettez en place une culture de «formation continue» et de partage des informations sur les risques cyber. Comprenez bien qu'il est impossible de se protéger à 100 % contre le risque cyber, ce qui rend d'autant plus indispensables les moyens de limiter ce risque, comme l'assurance cyber.

5.2 Le rôle de l'assurance cyber

1 Selon l'étude, 73 % des dirigeants d'entreprise n'ont qu'une connaissance limitée de l'assurance cyber et 50 % d'entre eux ne savent pas qu'il existe, en cas de fuites de données, des garanties couvrant les risques cyber.

2 L'assurance cyber garantit non seulement les versements de fonds après une attaque cyber mais donne aussi accès à des conseils d'experts afin d'améliorer la sécurité et l'assistance sur site pendant la période de crise.

3 Bien qu'il existe toute une gamme de polices cyber, elles ne couvrent généralement que deux types de coûts : les coûts de l'enquête technique et juridique visant à déterminer la cause et le ou les responsables de la fuite de données, ainsi que les coûts de communication aux clients et d'interruption des activités.

4 Travailler avec des assureurs qui comprennent bien ce type de risque dans son ensemble sera un avantage pour la stratégie de l'entreprise. Les assureurs peuvent aider les entreprises à identifier les risques et les failles et peuvent ainsi réduire dès le départ la probabilité d'une atteinte à la protection des données.

5 L'assurance cyber contribue non seulement à la protection des bilans de l'entreprise, mais aussi à l'augmentation de la sécurité informatique et à une meilleure gestion du risque.

Des fiches pays sont disponibles pour les pays suivants : Allemagne, Danemark, Espagne, France, Italie, Norvège, Pays-Bas, Royaume-Uni et Suède.

Pour plus d'informations et pour contacter un courtier du Lloyd's spécialisé dans le risque cyber, rendez-vous sur www.lloyds.com/cyber