Deloitte.

Enjeux Cyber 2016

La face cachée de la Cyber

Cyber

Sommaire

Introduction : avant-propos

Les discussions avec nos clients sont révélatrices : Comités Exécutifs, Directions métiers, DSI, RSSI, tous s'accordent à dire qu'un nombre important de sujets traités quotidiennement, touchent, appartiennent, impactent, ou sont impactés par la cybersécurité.

Toutefois, et comme le montre notre enquête, seulement 7%* des organisations considèrent la Cyber comme un sujet prioritaire et de premier ordre pour satisfaire la transformation digitale des entreprises. Les sujets de sécurité y sont traités à la marge et le cœur de l'activité de l'entreprise y est également délaissé.

L'exemple le plus flagrant peut être illustré lors de l'analyse des risques et de l'impact financier associé à une cyberattaque. Ce sont souvent les coûts directs en lien avec la perte ou le vol d'une information détenue par une entreprise (base de données clients par exemple) qui sont mis en avant alors que la destruction d'une infrastructure critique, la perte d'une propriété intellectuelle ou l'indisponibilité d'un système de production sont certes moins visibles pour le grand public mais peuvent causer des dommages financiers considérables.

C'est dans cette optique, et pour donner une vue la plus complète sur la cybersécurité et ces impacts de transformation, que cette étude « *Enjeux Cyber 2016* » a été réalisée. Elle vous révèle « *La face cachée de la Cyber* ». Sur la base d'une approche pluridisciplinaire, de notre connaissance de la cybersécurité et de notre expertise métier au niveau de l'ensemble des industries, nous illustrons les 5 enjeux incontournables de la Cyber qui touchent les organisations, avec à chaque fois les impacts visibles et non visibles.

Aborder la cybersécurité sous le prisme Métier/Business confère une meilleure vision quant aux stratégies à mettre en œuvre. Cela permet également de dépasser l'approche traditionnelle (orientée coûts directs) tout en encourageant à réfléchir au-delà de la « partie visible ».

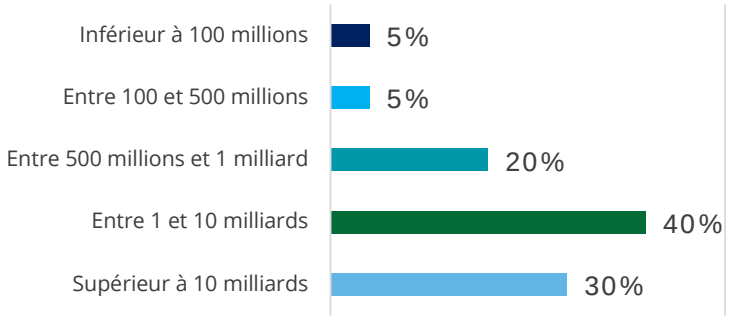
Michael Bittan
Associé responsable Cyber Risk Services
Deloitte France

(*) Toutes les données chiffrées de cette publication sont issues de l'enquête Cyber – Deloitte 2016.

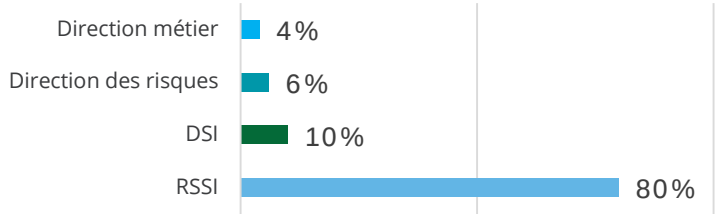
Méthodologie

Réalisée auprès de responsables de près de 40 organisations, cette enquête repose sur 12 questions portant sur la maturité de la cybersécurité dans les entreprises. Les deux graphiques ci-dessous présentent le profil des entreprises interrogées

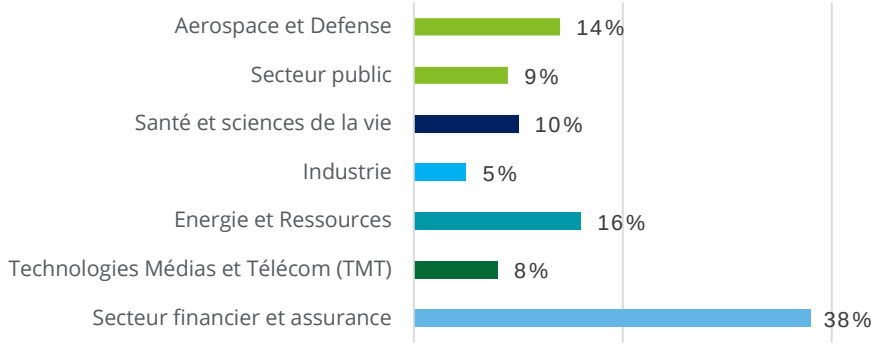
Répartition par chiffre d'affaires



Répartition par fonction



Répartition par secteur d'activité



1.

La transformation digitale

1. La transformation digitale

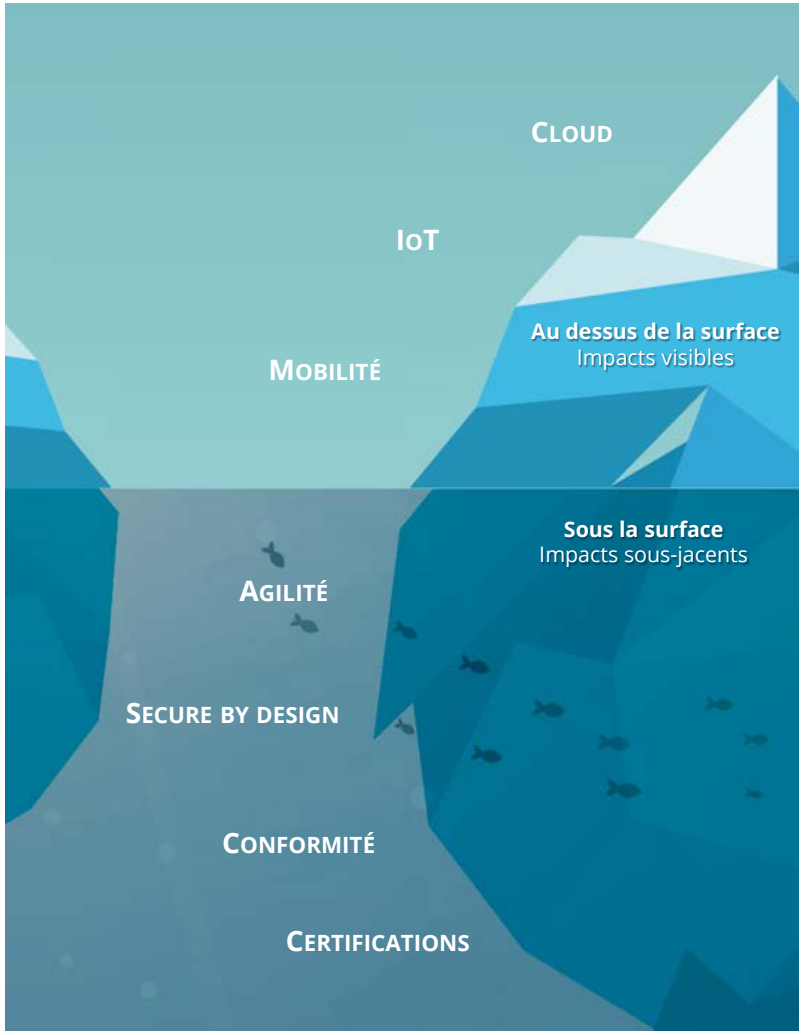
Cloud, SaaS, IoT, mobilité, Big Data…. la transition digitale modifie profondément et constamment le fonctionnement des entreprises, et les évolutions des modèles (infrastructures, communication, etc.) sont au cœur de cet enjeu de transformation.

Les concepts présentés ne restent toutefois que des moyens pour atteindre cette transformation dont l'ambition au sens plus large réside dans la mise en place d'une entreprise *agile* et rapide.

Dans un monde en constante évolution, la faculté d'une entreprise à mettre en place ou désactiver rapidement une plateforme répondant à un besoin est le critère recherché pour obtenir un avantage technologique et compétitif.

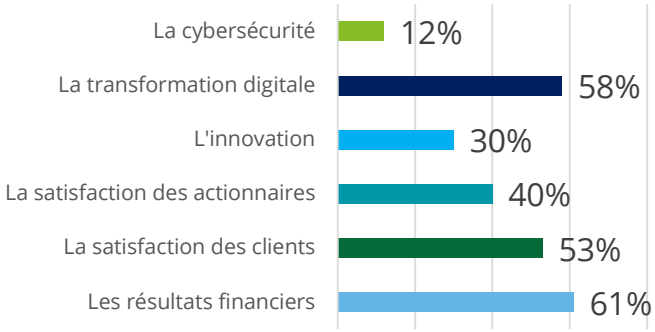
Dans ce contexte, les risques portés par la cybersécurité s'intensifient. Avec des délais toujours plus restreints, des technologies nouvelles, et des risques de failles de sécurité qui ne cessent de croitre, la mise en place de ce nouveau type de service est-elle suffisamment sécurisée ?

Tout particulièrement, les dispositifs de sécurité en lien avec les systèmes industriels (cible de plus en plus privilégiée des hackers) doivent être revus avec un monitoring accru des infrastructures industrielles, la réduction d'actions manuelles favorisant les cyberattaques mais aussi l'implication de spécialiste sur la question.

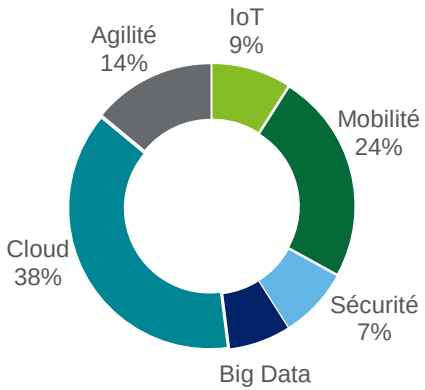


1. La transformation digitale

Quels sont les 3 enjeux prioritaires pour votre entreprise ?



Quel thème lié à la transformation digitale est considéré prioritaire par votre entreprise ?



Le saviez-vous ?

Sécurité, Auditabilité, Confidentialité, Disponibilité, Intégrité, Réversibilité, Localisation des données : comment s'assurer que ces critères soient remplis ? Avec des délais très courts et dans un environnement cloud où les entreprises possèdent de moins en moins d'infrastructures sous leur contrôle, cette assurance peut parfois s'avérer difficile à obtenir.

Les accompagnements, attestations et certifications **SOC2, PCI-DSS**, **ISAE3402** et **ISO2700X** sont autant de dispositifs qui permettent de se prémunir contre d'éventuelles failles et de garantir un niveau de sécurité adéquat pour le fonctionnement des nouveaux services proposés par l'entreprise. L'intégration de ces derniers points devient de plus en plus pris en compte par les fournisseurs Cloud.

Une approche *secure by design* est également primordiale pour se prémunir du mieux possible des cyberattaques. Dès les premières étapes de mise en œuvre d'un nouveau service (plateforme d'échanges entre clients et fournisseurs par exemple), les modèles et Framework utilisés ainsi l'architecture proposée doivent minimiser les impacts et réduire la possibilité de réaliser des actions malveillantes.

1. La transformation digitale

Cas pratique

Une entreprise a récemment mis au point un verrou connecté permettant à son possesseur de lister les personnes pouvant utiliser et débloquer le verrou tout en ayant une vision sur l'utilisation des accès octroyés.

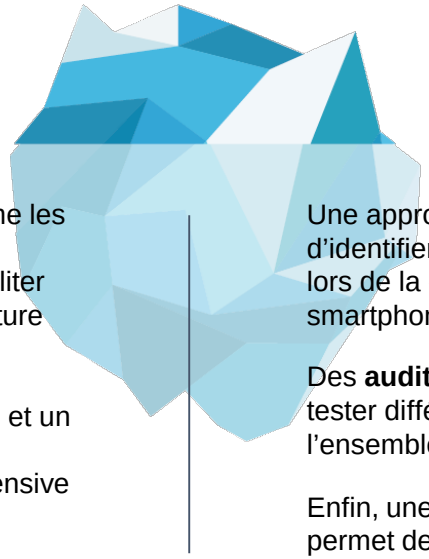
Des spécialistes en sécurité ont toutefois mis en évidence la facilité à récupérer les données de communication pour accéder au verrou.

Retour sur les faits

A LA SURFACE

L'objectif est alléchant : supprimer à terme les clés des serrures utilisées chaque jour (appartement, coffre, voiture, etc.) et faciliter l'**expérience utilisateur** avec une ouverture via le smartphone.

L'usage de cet **IoT** en lien avec le **Cloud** et un design épuré a été mis en avant par l'entreprise avec une communication intensive du service **Marketing**.



SOUS LA SURFACE

Une approche ***Secure by design*** aurait permis d'identifier que les clés virtuelles transitaient en clair lors de la communication Bluetooth entre le smartphone et la serrure.

Des **audits de sécurité** auraient également permis de tester différents types d'attaques (« force brute » : tester l'ensemble des combinaisons possibles, etc.).

Enfin, une **certification de type sécurité** du produit permet de s'assurer d'un bon niveau de fiabilité du verrou tout en donnant un avantage compétitif à l'entreprise car répondant aux attentes des clients.

2.

Les enjeux réglementaires

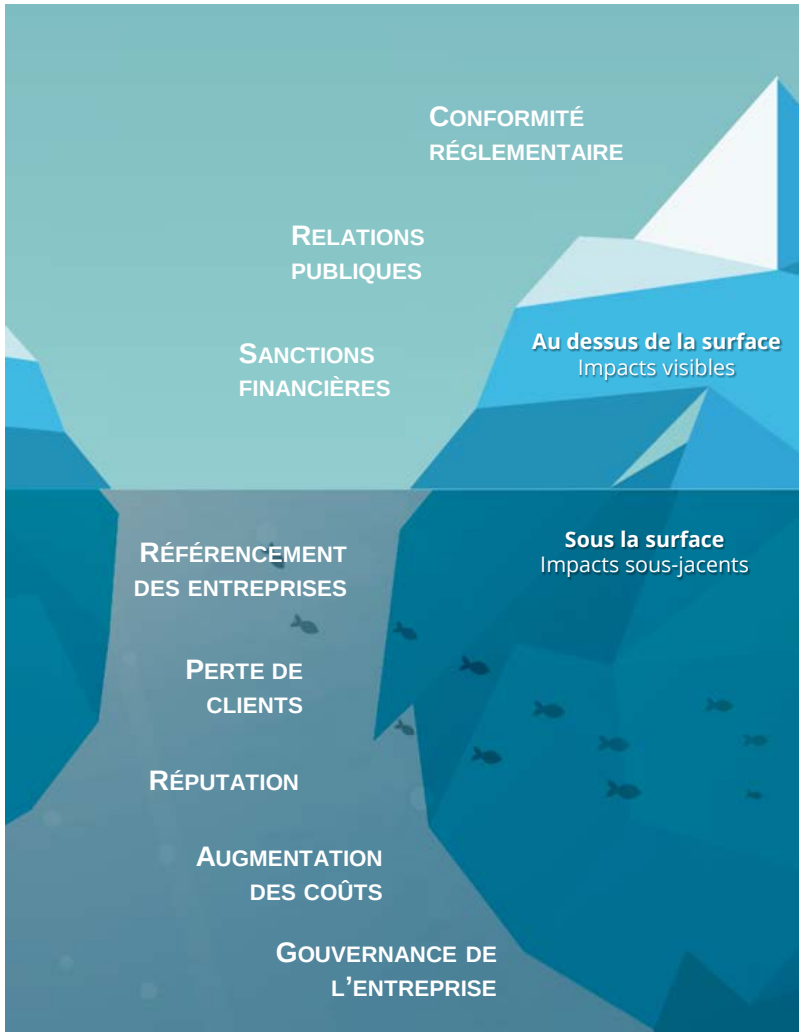
2. Les enjeux réglementaires

La question de la cybersécurité au niveau des entreprises se trouve à un tournant. L'intensification de la législation en Europe et en France introduit un changement de paradigme sur la question.

L'obligation réglementaire étant dorénavant introduite, les considérations actuelles des entreprises sur la cybersécurité (budget secondaire octroyé et consommé par la Direction des Systèmes d'Information ; approche risque informatique / constat / recommandation ; conseil exceptionnel suite à un incident) doivent être revues et corrigées.

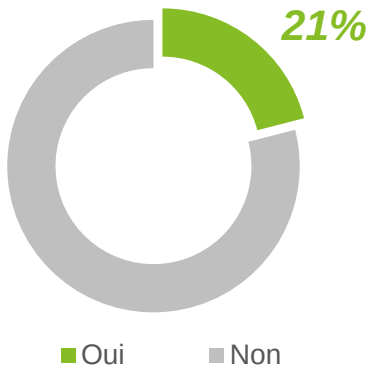
Le sujet devra dorénavant être porté et suivi de près par le management de l'entreprise avec une gouvernance clairement définie, en lien avec la stratégie de l'entreprise, et en accord avec la règlementation. Selon notre enquête, près de 25% des entreprises considèrent que la cybersécurité est un sujet porté par la Direction Générale.

L'enjeu est de taille, la conformité aux réglementations permettra aux entreprises de se prémunir de sanctions financières importantes pouvant avoir un impact considérable sur la réputation et la survie des entreprises. Les dispositifs de sécurité en périphérie des réglementations ne doivent toutefois pas être négligés.

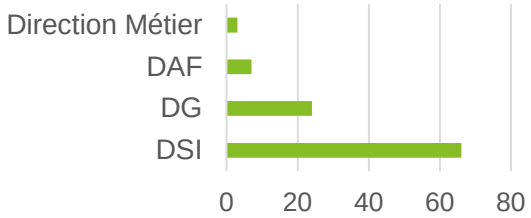


2. Les enjeux réglementaires

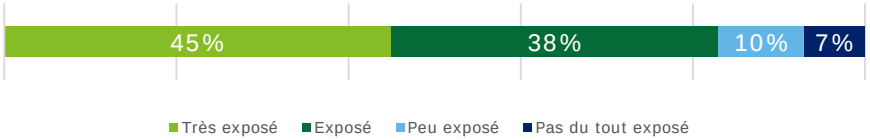
La cybersécurité fait-elle partie du Top 10 des priorités de votre entreprise ?



Quel est le département responsable de la cybersecurité au sein de votre entreprise ?



Comment qualifierez-vous votre niveau d'exposition aux cyberattaques ?



Le saviez-vous ?

La loi de programmation militaire (LPM) constitue, pour le ministère français de la Défense, la première étape de la mise en œuvre des nouvelles orientations stratégiques du Livre blanc sur la défense et la sécurité nationale. Cette réglementation concerne 200 entreprises classées « opérateurs d'importance vitale » (OIV). Ces OIV, réparties en 12 secteurs d'activités, exploitent des établissements ou utilisent des installations et ouvrages dont l'indisponibilité aurait un impact considérable sur la sécurité et le fonctionnement du pays.

A ce titre, les OIV sont tenus de :

- mettre en œuvre des systèmes qualifiés de **détection** des événements susceptibles d'affecter la sécurité de leur SI ;
- **alerter** sans délai le Premier ministre des incidents affectant le fonctionnement ou la sécurité de leur Systèmes d'Information d'Importance Vitale (SIIV) ;
- soumettre leurs SI à des **contrôles** réguliers destinés à vérifier leur niveau de sécurité.

L'**Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)** se chargera de réaliser les contrôles destinés à vérifier le niveau de sécurité et le **respect** des règles de sécurité prévues par la Loi. Des **dispositions pénales** à la fois pour les dirigeants et la personne morale sont prévues pour sanctionner les organismes qui manqueraient à leurs obligations.

2. Les enjeux réglementaires

Cas pratique

Une mutuelle de santé aux Etats-Unis a récemment fait face à un incident de sécurité majeur suite à la perte d'un ordinateur appartenant à un de ses collaborateurs.

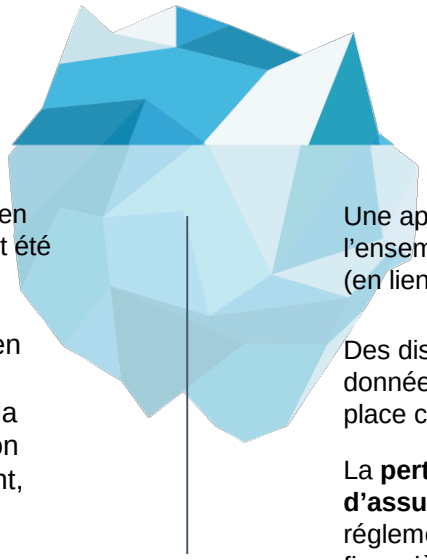
Malgré un dispositif de sécurité en place et répondant aux normes réglementaires du secteur de la santé aux Etats-Unis, des millions de données médicales ont été volées avec des conséquences importantes.

Retour sur les faits

A LA SURFACE

La mise en place de dispositifs de sécurité en lien avec les **réglementations** actuelles ont été une priorité pour la mutuelle.

Les éventuelles **sanctions financières** en cas de **non-conformité** ont incité les dirigeants à investir dans le domaine de la sécurité informatique : politique de gestion des accès, plan de reprise suite à incident, etc.



SOUS LA SURFACE

Une approche par les **risques** aurait permis d'identifier l'ensemble des menaces pouvant impacter l'organisation (en lien ou non avec la réglementation).

Des dispositifs de sécurité supplémentaires (chiffrement des données par exemple) auraient également dû être mis en place car l'impact financier était élevé.

La **perte des clients**, la **réputation** et les **coûts d'assurance** ont été négligés au détriment de la réglementation et se sont avérés plus impactant financièrement pour l'entreprise.

3.

La protection des données

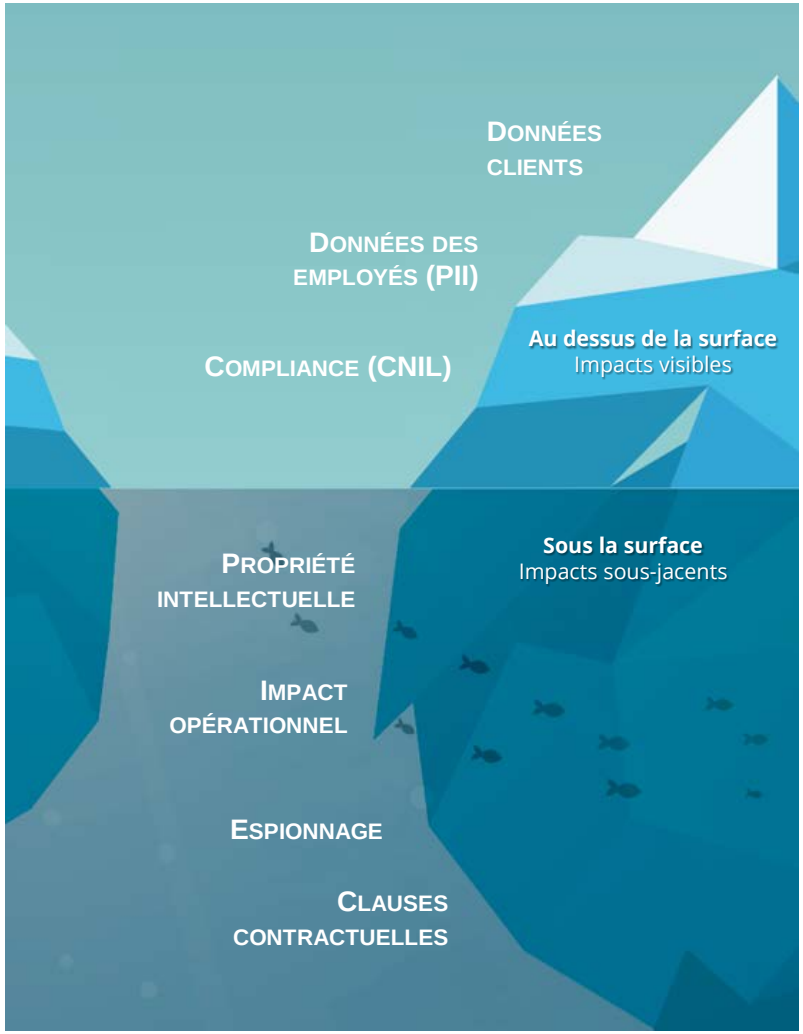
3. La protection des données

Le rapport entre la sécurité et la vie priée devient de nos jours critique. La récolte et l'enrichissement constante des données liées à une identité (employé, fournisseur ou client) conduit à faire du stockage des données sans consentement des individus et de l'éventuelle fuite de ces dernières un enjeu majeur.

En procédant à l'inventaire des données à disposition d'une entreprise, le risque ne s'arrête pas la. Les données personnelles, de paiement ou médicales (PII) sont les plus visibles et peuvent causer des impacts (amendes, réputation) que les entreprises ont bien intégré tout en mettant en place des dispositifs de contrôle.

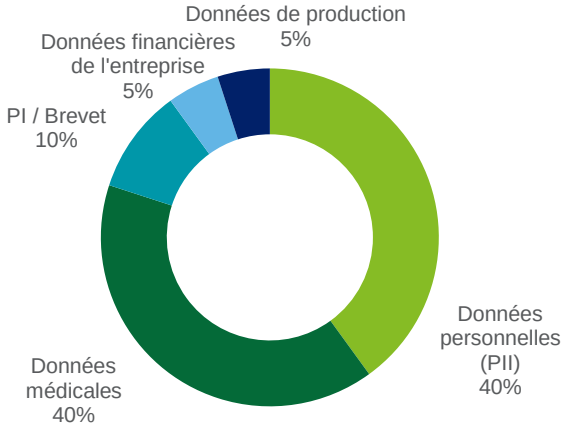
Cependant, les hackeurs ou personnes malveillantes n'ont pas toujours pour but le vol de données personnelles. L'espionnage, la propriété intellectuelle, la destruction de données ou l'altération d'infrastructure supportant des systèmes opérationnels ou industriels critiques sont également des scénarios pouvant avoir un impact très significatif sur les organisations.

Ces éléments ne sont pas souvent intégrés et doivent surtout faire l'objet d'estimation quantitative et qualitative pour classifier le risque et y répondre. A titre d'exemple, notre enquête révèle que les **données clients sont considérées comme critiques à hauteur de 40%** contre 10% pour les données de propriété intellectuelle.

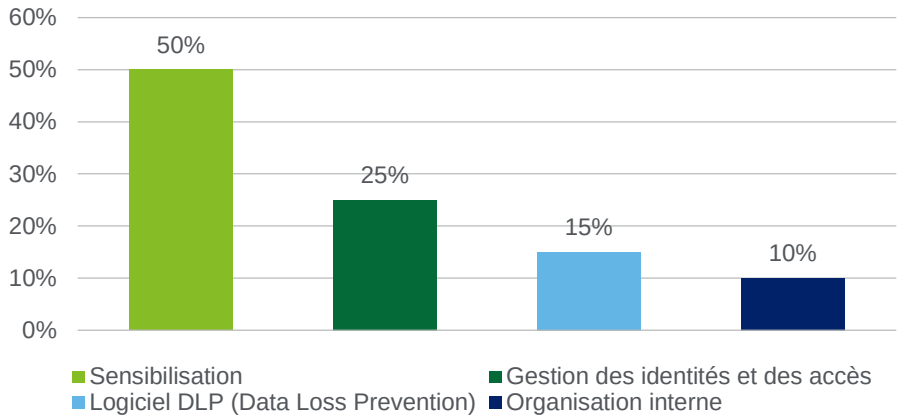


3. La protection des données

Quelles sont les données les plus critiques pour votre entreprise ?



Quelles sont les actions entreprises par votre organisation pour protéger les données ?



Le saviez-vous ?

Le nouveau règlement européen sur la protection des données personnelles appelé ***General Data Protection Regulation*** **(GDPR),** devra être appliqué d'ici deux ans par les entreprises.

Ce règlement concerne toutes les entreprises, administrations, collectivités locales et associations qui collectent, traitent et stockent des données personnelles dont les propriétaires peuvent être identifiés directement (par l'entreprise elle-même) ou indirectement (par un tiers). La plupart des sociétés sont donc concernées par ce nouveau règlement.

Concrètement que signifie l'entrée en vigueur du GDPR ? Le règlement oblige les organisations à s'assurer du **consentement explicite des individus** quant à l'utilisation qui sera faite de leurs données. Toutes les données doivent pouvoir être transférées à leur propriétaire ou effacées si ce dernier le demande. Le GDPR oblige également les organisations à être transparentes et à alerter les autorités compétentes en cas de constatation d'une fuite de données.

Enfin, la règlementation incite les entreprises à se doter d'une organisation interne en charge des questions relatives à la protection des données.

3. La protection des données

Cas pratique

Afin de faciliter la communication et l'échange de données avec ses clients, un cabinet d'avocats a déployé un portail web permettant l'échange de documents entre clients et avocats. Des mesures de sécurité avancées ont été introduites afin de protéger ce portail web et les données qui y transitent.

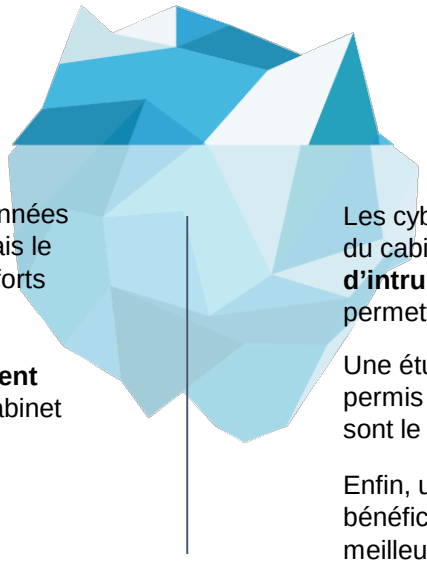
Une majeure partie des données de ce cabinet ont été volées et publiées sur internet.

Retour sur les faits

A LA SURFACE

La sécurisation du **portail web** avec les données qui y **transitent** était certes primordiale, mais le cabinet y a concentré l'ensemble de ses efforts en matière de sécurité.

La sécurité du **portail web** a été un **argument de vente** de taille qui a même permis au cabinet d'attirer de nouveaux clients.



SOUS LA SURFACE

Les cybercriminels ont contourné le portail et attaqué le SI du cabinet à travers son serveur de messagerie. Un **test d'intrusion** ou même un **scan de vulnérabilités** aurait pu permettre de déjouer cette attaque.

Une étude complète du **cycle de vie de la donnée** aurait permis d'identifier le moment et l'endroit où les données sont le plus exposées.

Enfin, une **certification** de type ISO 27001 aurait eu un bénéfice double : une meilleure **réputation** et une meilleure gestion de la sécurité.

4.

L’authentification

4. L'authentification

Les thématiques portées par l'**authentification** et de manière plus large la gestion des identités et des accès est également en constante évolution.

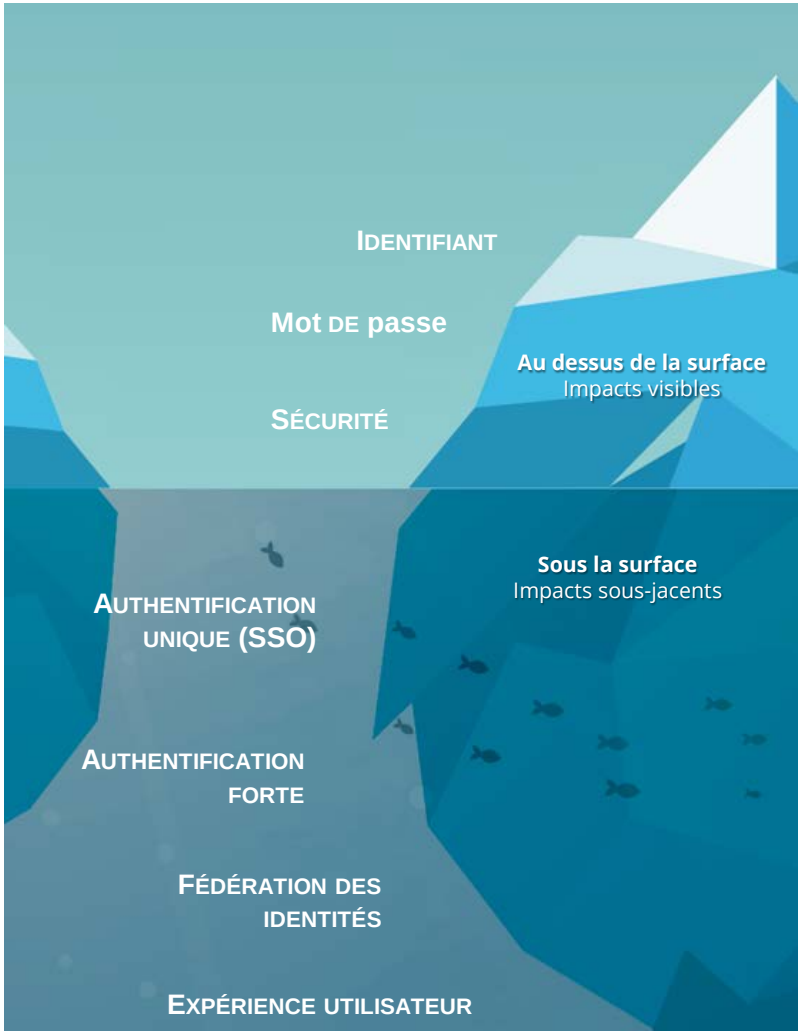
La problématique : permettre aux bonnes personnes d'accéder aux bonnes ressources d'entreprise au bon moment et pour la bonne raison, se voit peu à peu remplacer par : comment proposer à la fois un service sécurisé tout en augmentant l'expérience utilisateur.

Les organisations utilisent encore aujourd'hui des applications métiers proposant à chaque fois des identifiants et mots de passe différents. C'est une vraie peine pour les employés dont l'alternative consiste à stocker les dizaines d'identifiants ou mots de passe sur un Post-it ou sur un fichier accessible à partir du premier écran de l'ordinateur.

L'identité numérique est au cœur du sujet. Disposer d'une identité digitale unique et centralisée, interagissant avec l'ensemble du système d'information de l'entreprise est la pierre angulaire d'un dispositif de sécurité.

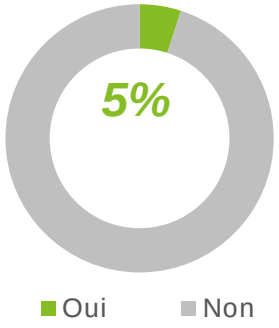
Pour les applications critiques des entreprises, la sécurité est à privilégier avec l'**authentification forte** (MFA – Multi Factor Authentication) qui permet de valider l'identité des utilisateurs en proposant une alternative complémentaire au mot de passe (par exemple, un mot de passe : *ce que l'on connait* avec une empreinte digitale : *ce que l'on est* ; ou encore un mot de passe *: ce que l'on connait* avec un code reçu sur son smartphone : *ce que l'on possède*).

Pour les autres systèmes moins critiques, l'expérience utilisateur est à privilégier avec l'authentification unique (SSO – Single Sign On) qui permet aux utilisateurs de s'authentifier une seule fois (mot de passe de l'ordinateur par exemple) pour toute la durée de la session, et ce indépendamment des autres applications utilisées.

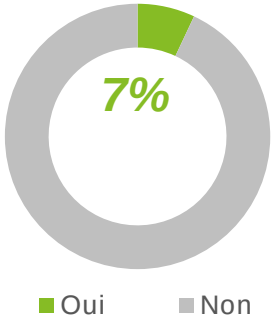


4. L’authentification

Votre entreprise utilise-t-elle la Biométrie comme mécanisme d’authentification ?



Votre entreprise utilise-t-elle la fédération des identités ?



Le saviez-vous ?

Face à la nécessité de devoir constamment s’authentifier et saisir des mots de passe différents pour chaque application ou service, la **fédération des identités** apporte une solution efficace permettant une authentification et propagation transparente des données entre applications.

L’utilisation de fournisseurs d’identité tel que Facebook, Google, Twitter, etc. permettent, par l’intermédiaire de la création d’un profil « social », d’associer l’identité aux nouveaux services proposés pour ainsi éviter la gestion multiples des mots de passe.

La **biométrie** se démocratise également de plus en plus. L’identification rapide des utilisateurs de smartphone par l’intermédiaire de leur empreinte digitale a permis une adoption assez large de cette technologie.

Elle n’est toutefois utilisée que chez 5% des clients de notre enquête.

Une fois les problématiques de stockage, protection et utilisation de ces données correctement adressées, cette technologie (qui commence à être de plus en plus utilisée par les banques pour l’identification des utilisateurs) permet d’introduire une sécurité accrue des services tout en améliorant l’expérience utilisateur.

4. L’authentification

Cas pratique

Un fournisseur de messagerie en ligne a profité de l’essor d’internet dans certains pays pour obtenir une base d’utilisateurs importante. Une connexion classique avec un identifiant et un mot de passe est en place mais les aspects de sécurité ont été négligés.

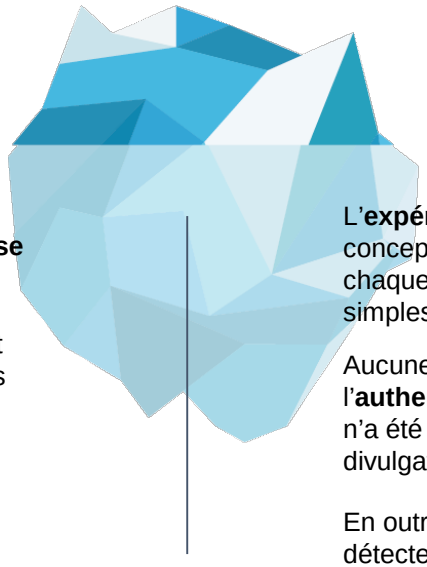
Ce fournisseur de messagerie a vu sa base de données identifiants/mots de passe en clair se faire dérober.

Retour sur les faits

A LA SURFACE

Le fournisseur requiert une authentification basée sur un **identifiant** et un **mot de passe** sans aucune complexité.

Le stockage des données étaient en clair et facilement accessible. A titre d’exemple, les mots de passe les plus utilisés étaient : « asdasd » ou encore « 000000 ».
.



SOUS LA SURFACE

L’**expérience utilisateur** a été négligée lors de la conception de la solution (ressaisie du mot de passe à chaque connexion) incitant l’utilisation de mots de passe simples.

Aucune solution alternative d’authentification telle que l’**authentification forte** ou l’**authentification unique (SSO)** n’a été envisagée pour la messagerie, ce qui rend la divulgation des mots de passe critique.

En outre, un simple **audit de sécurité** aurait permis de détecter que les mots de passe étaient en clair dans la base avec une complexité faible.

5.

L’évidence Cyber

5. L'évidence cyber

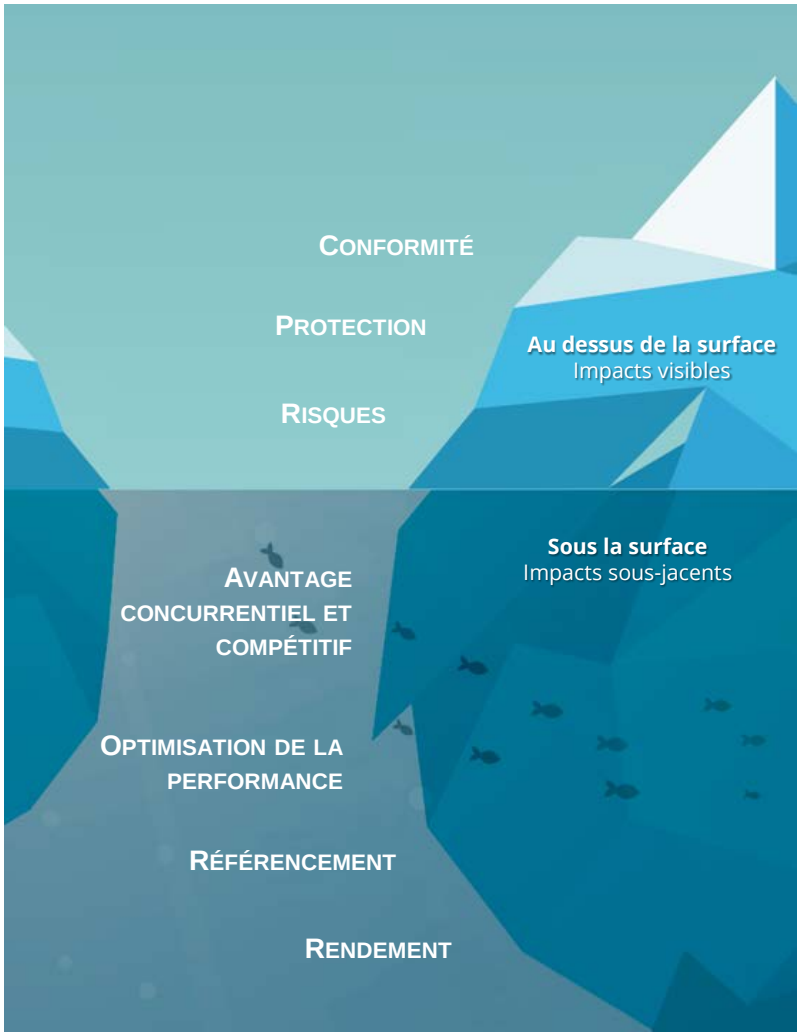
Deux visions s'opposent. L'approche traditionnelle vise à traiter les risques Cyber dans le but de les maitriser et supprimer. Les mesures prises par l'entreprise permettent de mieux se protéger contre d'éventuelles attaques tout en répondant aux contraintes des régulateurs.

Pour d'autres, et c'est une approche totalement différente, la cybersécurité est une chance. Des avantages considérables peuvent en être tirés puisqu'une gestion intelligente de ces risques aboutira à une amélioration du rendement et à une optimisation de la performance.

C'est donc dans cette optique que les entreprises doivent envisager la cybersécurité. Dans un environnement en constante transformation où les entreprises deviennent de plus en plus exposées aux risques mais également à la concurrence, une meilleure appréhension des dispositifs de sécurité à mettre en place fournira un avantage compétitif de taille par rapport aux autres.

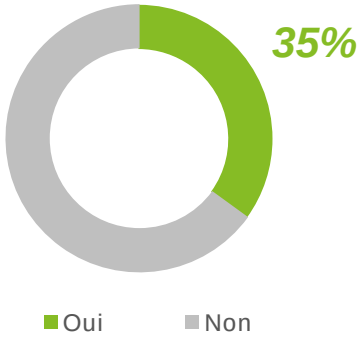
Les décisions stratégiques des entreprises pourront être réalisées sereinement dans le sens où la gestion des risques qui y est associée (identification, évaluation, réponse) sera non seulement orientée « protection » mais également « optimisation de la performance ».

A titre d'exemple, les entreprises ayant par le passé décidé de mettre en place une stratégie Cyber se voient aujourd'hui récompensées puisque de plus en plus de clients exigent de leur fournisseur l'existence de dispositifs de sécurité avant d'envisager une collaboration (ordinateurs sécurisés, plateforme d'échanges de données cryptées, etc.)

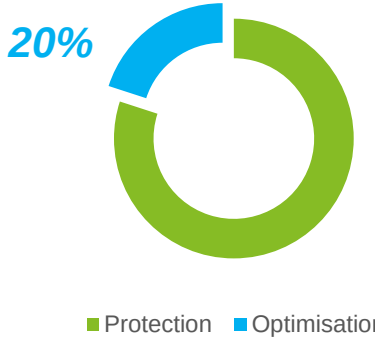


5. L'évidence cyber

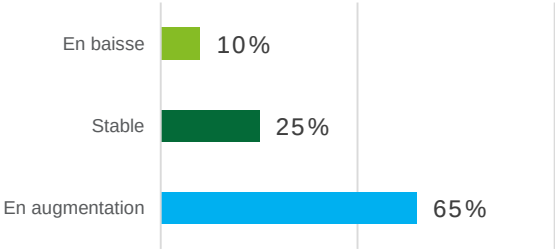
Vos stratégies d'entreprise prennent-elles en compte l'enjeu Cyber ?



Sur quoi une bonne gestion des risques de cybersécurité doit-elle se concentrer en priorité ?



Votre budget consacré à la cybersécurité pour l'année prochaine sera :



Le saviez-vous ?

Le point d'équilibre à trouver entre protection et optimisation ne doit pas s'arrêter la. Le développement des entreprises passant par une innovation constante et nécessaire devra pleinement s'exprimer d'un point de vue sécurité avec le marketing de la fonction Cyber et des RSSI.

En termes de communication, mais en contribuant aussi aux projets stratégiques des entreprises, la fonction Cyber permettra d'accompagner sereinement les entreprises dans leurs transformations. Les bénéfices traditionnels tels que protéger les actifs ou contrôler les accès seront complétés par des apports considérables au niveau de l'augmentation de la productivité, la mise en place de nouveaux modes d'interaction et de ruptures technologiques autour de la mobilité et de la collaboration.

Conclusion

En guise de conclusion, la prise en compte des enjeux Cyber ainsi que la mise en place d'une stratégie Cyber doit toutefois être mis en relief par rapport à l'affirmation suivante :

Le risque zéro n'existe pas en informatique : certaines cyberattaques ne peuvent pas être évitées mais l'impact associé peut être maitrisé.

L'approche traditionnelle qui consiste à traiter la sécurité IT comme un risque inhérent à chaque entreprise est dépassée. Le triptyque « Sécurité – Vigilance – Résilience » permet de répondre aux enjeux proposés:

Ce qui compte pour l'entreprise

Une analyse de ce qui compte réellement pour l'entreprise doit aboutir à des investissements et mesures permettant de sécuriser les actifs identifiés et réduire l'impact potentiel des menaces.

Réduire les cyber-attaques

La sensibilisation et le monitoring sont les meilleures protections. Cela permet en effet d'obtenir une meilleure connaissance des menaces et identifier lorsqu'elles se produisent ou sont sur le point de se produire pour mieux les traiter.

Quel réponse suite à une attaque

La réduction de l'impact est certes la première étape. La capacité de l'entreprise à se remettre en marche rapidement sans perte d'information ou avec le moindre des préjudices est tout aussi important.

Conclusion

Pour chaque organisation, une stratégie de réponse à la Cyber autour de l'approche « Sécurité – Vigilance – Résilience » doit également prendre en compte les deux aspects suivants :

Mettre en place la bonne équipe

Une compréhension collective du métier, de la stratégie de l'entreprise, des processus, des contraintes réglementaires, des opérations et des technologies utilisées permettra d'identifier ce qui compte pour l'entreprise, les risques les plus importants à adresser, les biens les plus précieux à protéger, mais surtout quels sont les impacts à maitriser.

Rendre la Cyber visible

Cette étude se propose de faire la lumière sur l'ensemble des enjeux que proposent la Cyber.

Bien que non visible, un incident technique peut parfois s'étendre et toucher le cœur du métier de l'entreprise pour finalement avoir un impact considérable.

En adoptant une approche de la sorte et à travers ce prisme, nous avons la conviction que les entreprises seront les mieux à même de répondre et prospérer face au nombre croissant de cyberattaques.

Contrôler les investissements

C'est un fait, les budgets sont et ne seront jamais suffisamment élevés pour se prémunir de l'ensemble des risques. Même si des investissements plus importants sont parfois nécessaires, l'effort doit avant tout se concentrer sur la réduction de l'impact que peut occasionner un incident.

Auteurs

Michael Bittan
Associé responsable Cyber Risk Services
Deloitte France

Fouzi Akermi
Manager Cyber Risk Services
Deloitte France

Deloitte.