Deloitte.

Enjeux Cyber 2018

L'évolution de la menace Cyber

Cyber

Janvier 2018

Editorial

Après des années où les entreprises se sont posées la question de la pertinence de leurs investissements sur les sujets en lien avec la cybersécurité, l'année 2017 a marqué un tournant pour les raisons suivantes :

- Des attaques mondiales et majeures ont éclaté, touchant un grand nombre d'entreprises. L'impact médiatique de ces attaques a été sans précédent.
- L'intensification de la réglementation pour la protection des données personnelles (avec en point de mire le RGPD : règlement général sur la protection des données) ou la sécurisation des systèmes d'information s'est imposée au sein des entreprises, lesquelles ont, dans une grande majorité, pris les mesures adéquates.

L 'enquête menée auprès de nos clients affiche clairement ces tendances, ainsi qu'une volonté d'agir face à l'évolution de la menace Cyber. Appréhender cette activité comme une composante à part entière de l'entreprise, complétement intégrée au métier et au besoin technologique et d'innovation, permettra d'en prendre pleinement la mesure, afin d'y apporter des réponses appropriées.

71%

des entreprises affirment que le nombre de cyberattaques à leur encontre est en hausse

Rétrospective de l'année 2017 et perspectives pour 2018

Que s'est-il passé en 2017 ?

- Des attaques massives ayant impacté et paralysé de nombreuses entreprises (Wannacry, Petya)
- Des fuites de données personnelles (données clients et salariés) qui ont, cette année encore, touché les entreprises
- Une réglementation de plus en plus présente (RGPD, LPM, DSP2) avec des mesures de sécurité dorénavant obligatoires pour chaque entreprise

Que nous réserve 2018 ?

- Une pression accrue des régulateurs avec une forte probabilité de sanctions (amendes significatives en guise d'exemple)
- La généralisation des assurances en lien avec les risques de cyberattaques
- Le renforcement du concept « Secure by Design » avec la prise en compte des mesures de sécurité pour toute tendance innovante (IoT, Blockchain) ou toute composante métier (industrie, finance, RH, télécoms, consommation, etc.)

Deux constantes toutefois à noter : les **investissements** et l'**intérêt des organisations** pour la cybersécurité sont **en augmentation**.

Sommaire

La généralisation des cyberattaques

La généralisation des cyberattaques

- Notre précédente étude se proposait de lister les cyberattaques les plus fréquentes recensées par nos clients. Ransomwares, phishing et autres cybermenaces étaient généralement estimées par des coûts directs (mise en conformité, interruption de service, etc.) sans la prise en compte des coûts indirects tels que la perte de confiance des clients ou la dépréciation de l'image de marque.
- L'actualité de cette année vient rappeler à quel point les menaces et les impacts (directs ou indirects) associés sont toujours à l'ordre du jour, 71% de nos clients confirmant la hausse du nombre de cyberattaques dont ils font l'objet.
- Il a fallu cependant des attaques mondiales comme Wannacry ou Petya pour que les entreprises réagissent. 75% des entreprises affirment avoir pris des mesures de sécurité supplémentaires pour renforcer leurs systèmes d'information suite à ces événements.

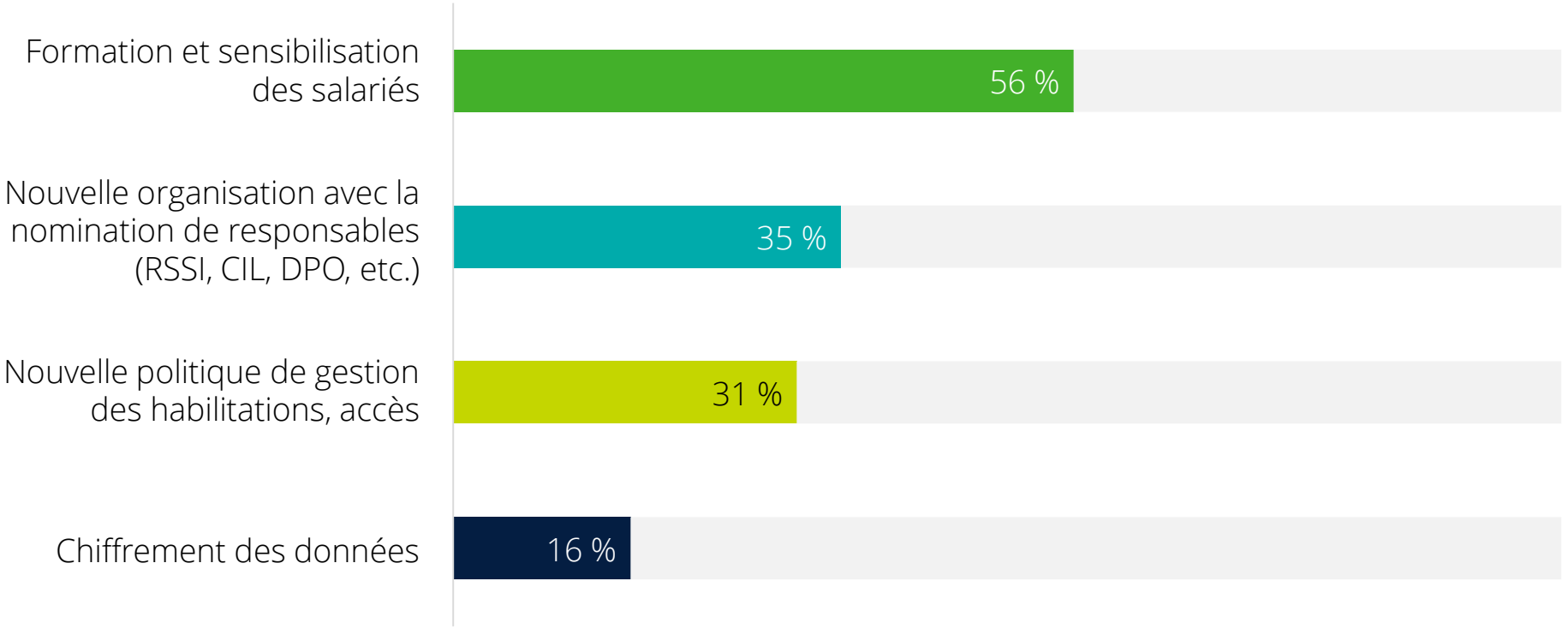
75%

des entreprises ont adopté de nouvelles mesures de sécurité en lien avec les récentes attaques (Wannacry, Petya)

- La formation et la sensibilisation des collaborateurs, tout comme la gestion des accès, sont autant de mesures peu onéreuses qui permettent un gain considérable face à la cybercriminalité croissante.

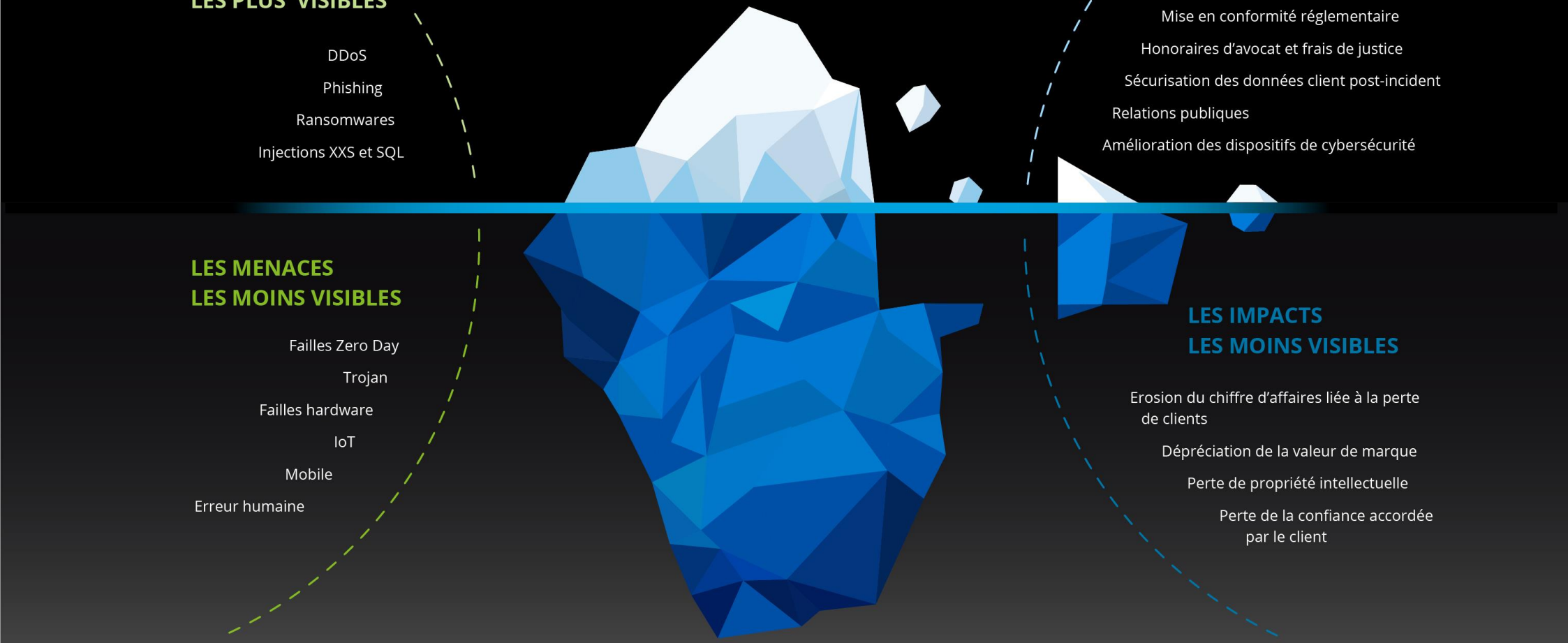
La généralisation des cyberattaques

Les nouvelles mesures de sécurité mises en place par les entreprises suite aux récentes attaques (Wannacry, Petya)



La généralisation des cyberattaques

Plus que jamais le panorama des menaces est un inventaire utile que les entreprises doivent avoir en tête pour la mise en place de mesures de protection. A ce panorama s'ajoutent les coûts directs et indirects qui interviennent en cas d'accident de sécurité liés à une cyberattaque, pour une meilleure réponse.



LES MENACES LES PLUS VISIBLES

- DDoS
- Phishing
- Ransomwares
- Injections XXS et SQL

LES IMPACTS LES PLUS VISIBLES

- Enquêtes techniques
- Notification client de l'intrusion
- Mise en conformité réglementaire
- Honoraires d'avocat et frais de justice
- Sécurisation des données client post-incident
- Relations publiques
- Amélioration des dispositifs de cybersécurité

LES MENACES LES MOINS VISIBLES

- Failles Zero Day
- Trojan
- Failles hardware
- IoT
- Mobile
- Erreur humaine

LES IMPACTS LES MOINS VISIBLES

- Erosion du chiffre d'affaires liée à la perte de clients
- Dépréciation de la valeur de marque
- Perte de propriété intellectuelle
- Perte de la confiance accordée par le client

Les cyberassurances contre les cybermenaces

Les cyberassurances contre les cybermenaces

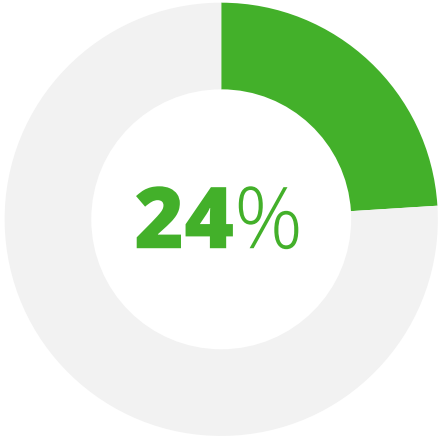
La généralisation des cyberattaques suppose dorénavant d'appréhender la cybersécurité sous un autre angle. Le risque zéro n'existant pas, les répercussions d'une cyberattaque doivent être traitées sous deux aspects :

- Quelle réponse à un incident l'entreprise doit-elle apporter à court, moyen et long terme pour un rétablissement durable de l'activité ?
- Quelles sont les assurances à souscrire pour couvrir les éventuels dommages ?

Aujourd'hui, seulement 24% des entreprises sondées ont souscrit à une assurance en lien avec les risques de cybersécurité.

Le vieil adage « Ce qui ne peut pas être protégé peut être assuré » fait complétement sens, et de plus en plus d'entreprises intègrent le risque de cyberattaques dans leurs contrats d'assurance pour minimiser l'impact financier suite à un incident.

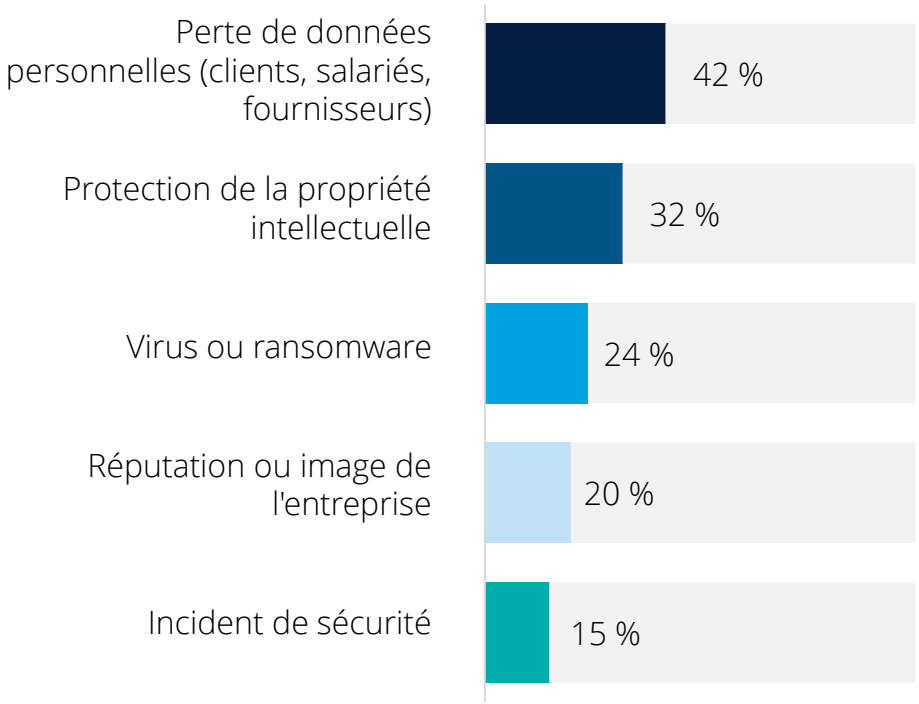
Souscrire à une cyberassurance permet également à l'entreprise d'effectuer une évaluation préalable de son niveau de risque de sécurité pour ainsi connaître son niveau de maturité et les différentes vulnérabilités de son système d'information. Cette évaluation, pleinement partagée avec le métier, permettra d'appréhender l'écosystème informatique d'un point vue cybersécurité (données personnelles, réglementation, accès, etc.) et de bénéficier ainsi de la meilleure assurance.



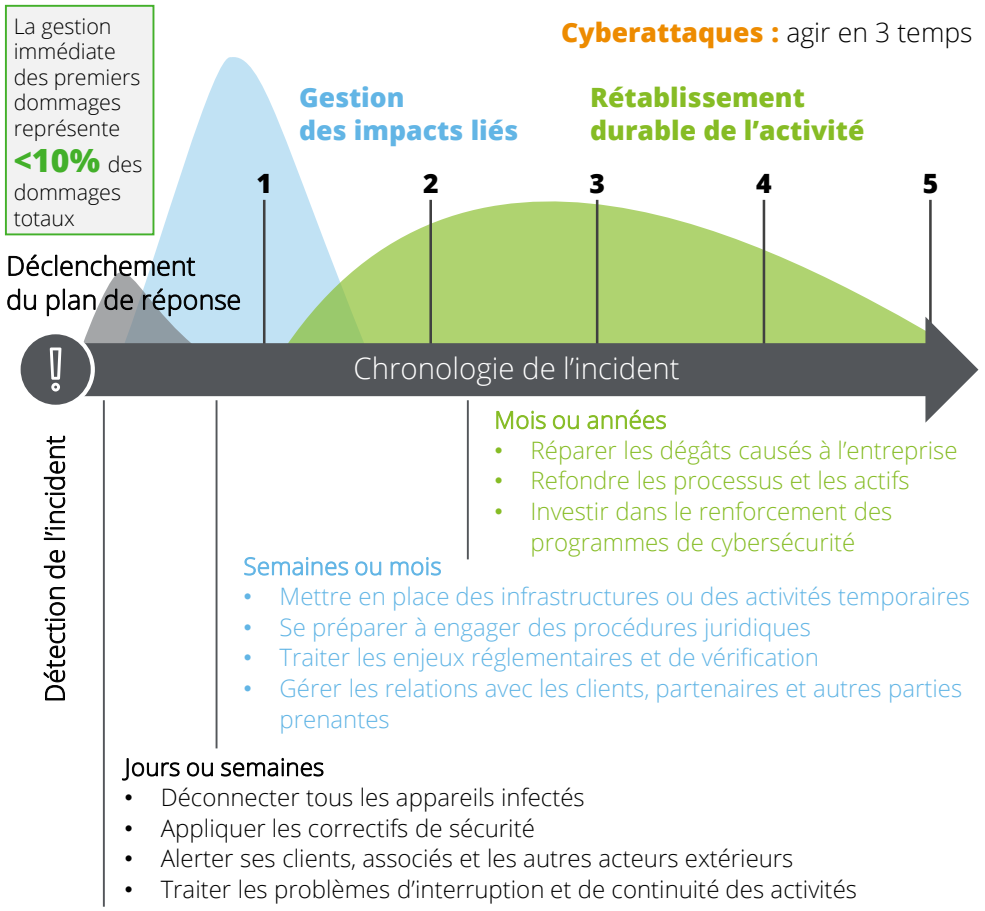
des entreprises ont souscrit à une assurance pour se prémunir des risques de cybersécurité

Les cyberassurances contre les cybermenaces

Répartition des options de couverture des risques lorsqu'une assurance est souscrite



Aucune assurance ne pouvant protéger pleinement l'image de marque en cas de cyberattaque, il est également nécessaire de rappeler les mesures à mettre en place par l'entreprise afin de rétablir son activité dans les meilleurs délais.



L’humain au cœur de la cybersécurité

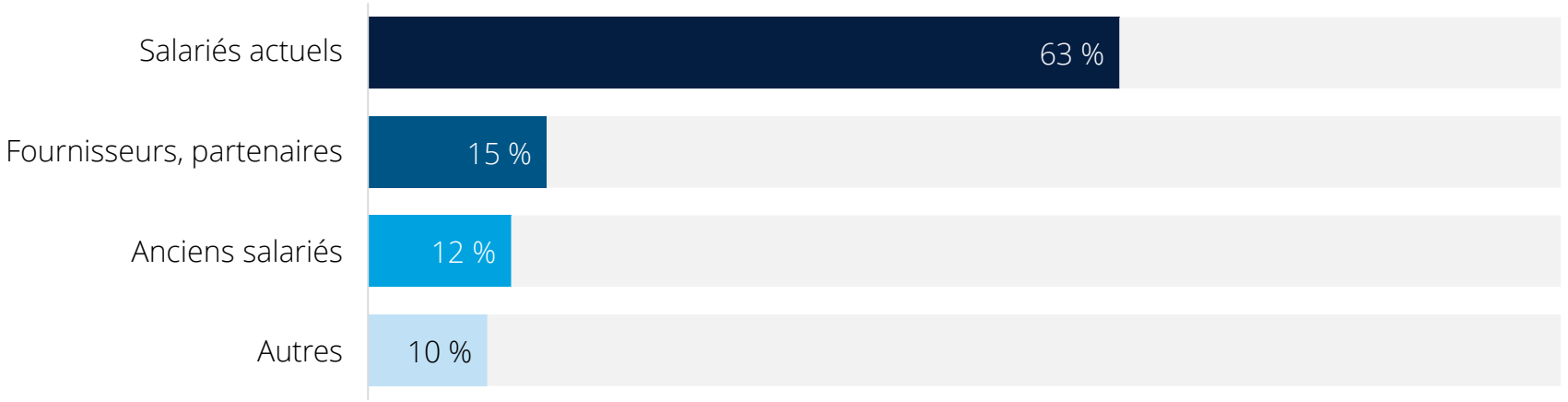
L’humain au cœur de la cybersécurité

Gestion des collaborateurs

Le constat est sans appel. Notre enquête auprès de nos clients révèle que 63% des incidents de sécurité proviennent d’un collaborateur actif au sein des effectifs. En effet, le système informatique hautement sécurisé d’une entreprise peut être mis à mal très rapidement par une action malintentionnée ou une erreur de la part d’un salarié.

Les dégâts susceptibles d’être provoqués par une personne en interne peuvent être considérables si la politique de gestion des identités et des accès n’est pas optimale. Il est primordial de s’assurer que chaque collaborateur ne possède pas de droit d’accès étendu non nécessaire, mais également d’évaluer les actifs informationnels les plus critiques pour mieux les sécuriser.

Répartition de la source des incidents de sécurité liés à l’humain



L’humain au cœur de la cybersécurité

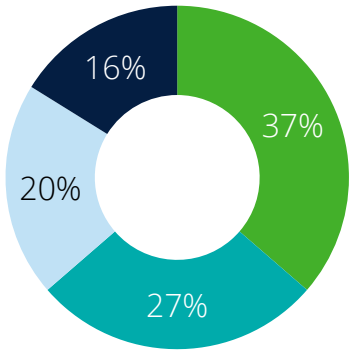
Gestion et formation des talents

Afin de mieux sécuriser son système d’information, il est nécessaire de disposer d’experts en cybersécurité qui seront à même de conduire les programmes de sécurité au sein de l’entreprise (politique, procédure, outils, sensibilisation, etc.).

Le recrutement, la formation et la rétention des talents sont, certes, des problématiques d’actualité chez les entreprises mais elles sont d’autant plus accentuées lorsqu’il s’agit de la cybersécurité pour les deux aspects suivants :

- la faible disponibilité des experts en cybersécurité au regard de la forte demande des entreprises souhaitant recruter et se renforcer massivement sur ce secteur ;
- la formation, la mise à jour et donc la rétention constante de ces experts, une fois recrutés, sur la nature des nouvelles cybermenances et les approches innovantes de sécurité associées.

Répartition des problématiques liées à la rétention des talents en cybersécurité



- Identification et sélection des formations adéquates
- Opportunités ne répondant pas aux attentes des professionnels de la cybersécurité
- Possibilité de proposer des formations qui intéressent les professionnels de la cybersécurité
- Risque de départ à la concurrence

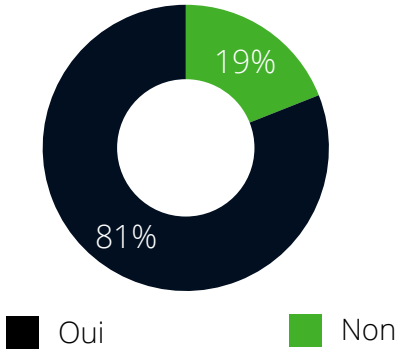
L’humain au cœur de la cybersécurité

L’implication des Directions

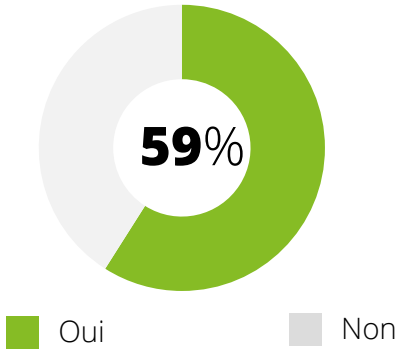
Une bonne politique de gestion de la cybersécurité pour une entreprise reposera sur l’implication du management pour définir les rôles et responsabilités adéquats (RSSI, DPO, CIL, etc.) mais aussi pour initier les programmes de sensibilisation et formation des salariés. Plus spécifiquement, les actions suivantes peuvent être entreprises :

- création d’une fonction de type « RSSI » transverse à l’ensemble de la société qui sera responsable des programmes/sujets en lien avec la sécurité. C’est déjà le cas pour 81% des entreprises sondées ;
- mise en place d’e-learnings ou de sessions de formation à destination de tous les collaborateurs pour les aider à mieux identifier les potentielles attaques et menaces (phishing, ransomwares, etc.) ;
- adoption d’un dispositif de gestion du risque Cyber par l'intermédiaire d'un cadre de type ISO 27001. C’est déjà le cas pour 59% des sondés.

Votre RSSI est-il en charge du programme de sécurité globale pour votre entreprise ?



Votre entreprise a-t-elle mis en place un dispositif de gestion du risque Cyber par l'intermédiaire d'un cadre déjà éprouvé (ex. : ISO27001) ?



Les technologies au service de la cybersécurité

Les technologies au service de la cybersécurité

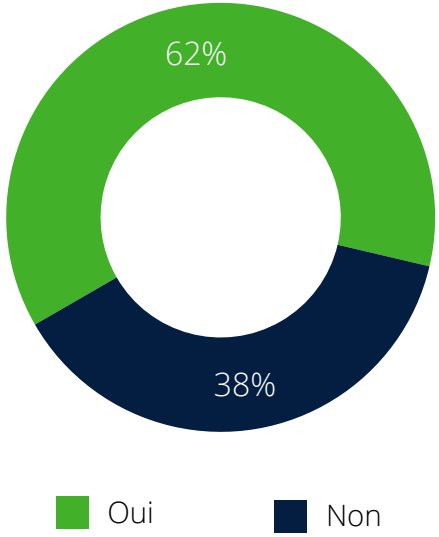
A l'heure où les menaces de cyberattaques sont de plus en plus présentes avec des typologies d'attaques en constante évolution, les entreprises doivent dorénavant repenser leur outillage et introduire des fonctionnalités nouvelles et à la pointe de la technologie :

On identifiera entre autres :

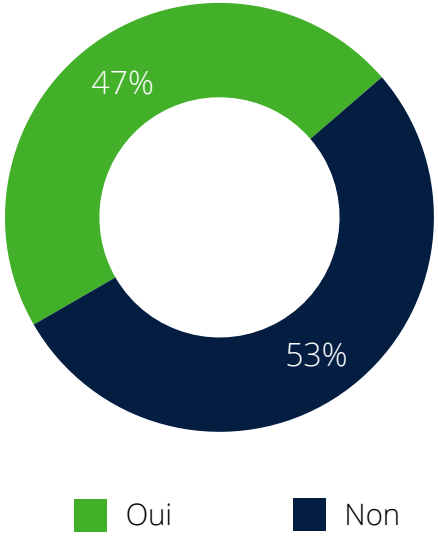
- Des services de sécurité sur la base de solutions Cloud et en mode SaaS
  - Les fournisseurs Cloud proposent de plus en plus de garantie en termes de sécurité et de protection des données. L'utilisation d'une architecture Cloud permet également des capacités de stockage et de traitement de données très importantes et nécessaires pour la gestion des événements de sécurité.
- L'utilisation de la Data pour la prédiction de cyberattaques
  - Son utilisation est encore faible chez les entreprises mais son pouvoir peut être très intéressant, notamment pour le monitoring des menaces et la prédiction des attaques, mais aussi pour la réponse à un incident avec l'analyse et l'audit des logs. Les entreprises et éditeurs de logiciels pensent également à utiliser l'Intelligence Artificielle pour rendre la prédiction de cyberattaques plus efficace et introduire des actions de remédiation en temps réel pour stopper l'incident.
- L'authentification forte
  - Le mot de passe seul n'étant plus une solution, des moyens alternatifs pour se connecter aux applications et données critiques sont à l'ordre du jour. L'utilisation d'un deuxième facteur d'authentification (sms, biométrie, etc.) pour la connexion des salariés ou tiers (fournisseurs, clients) permet de réduire significativement le risque de fraude tout en améliorant l'expérience utilisateur.

Les technologies au service de la cybersécurité

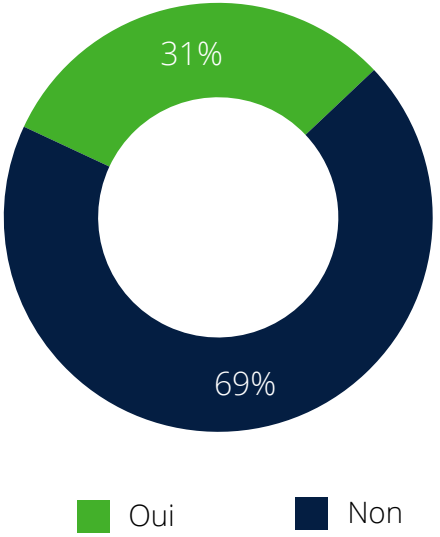
Taux d'utilisation du Cloud pour les outils de cybersécurité



Utilisation de la Data dans le cadre du monitoring des logs d'événements de sécurité



Utilisation de l'authentification forte pour l'accès aux applications sensibles



Les nouvelles règles face aux nouveaux risques

Les nouvelles règles face aux nouveaux risques

Le renforcement significatif des contraintes réglementaires est fortement lié à la généralisation des cyberattaques et des fuites de données au sein des entreprises.

Au fil des années, directives et autres normes ont vu le jour et font désormais partie du paysage et des dispositifs à mettre en place pour satisfaire les exigences et éviter de se voir infliger de lourdes amendes. Rappelons les principales réglementations en vigueur :

RGPD (Règlement Général sur la Protection des Données) Date d'entrée en vigueur : 25 mai 2018

- Ce nouveau règlement européen oblige les organisations à s'assurer du consentement explicite des individus quant à l'utilisation qui sera faite de leurs données. La transparence, la mise en œuvre d'alerte en cas de constatation d'une fuite de données, mais également la mise en place d'une structure interne dédiée à la protection des données sont notamment exigées.

LPM (Loi de Programmation Militaire)
Date d'entrée en vigueur des mesures de cybersécurité : Juillet 2016

- Cette réglementation concerne les entreprises classées « Opérateurs d'Importance Vitale » (OIV) qui sont tenues de renforcer leur niveau de sécurité (contrôles réguliers, détection des événements, alerte suite à un incident) sous peine de dispositions pénales. La directive européenne NIS, dans le même registre, est également à prendre en considération.

DSP 2 (Directive sur les services de paiement 2)
Date d'entrée en vigueur : 13 janvier 2018

- Cette directive européenne définit les règles concernant les nouveaux acteurs sur le marché des paiements (FinTechs). Les services d'agrégation d'information (permettant une vision consolidée des comptes bancaires) ou les services d'initiation de paiement sont dorénavant encadrés et des mesures de sécurité exigées (sécurisation des API, authentification forte, etc.).

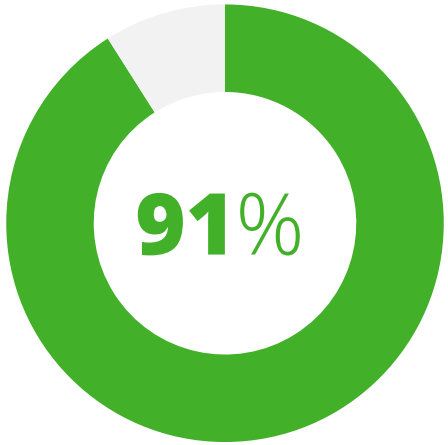
Programme sécurité de SWIFT
Date d'entrée en vigueur : Janvier 2018

- Un ensemble de standards de sécurité qui devient obligatoire pour tous les membres du réseau. Chaque membre SWIFT sera tenu de publier une auto-attestation annuelle faisant état du respect des points de contrôle obligatoires (sécurisation de l'environnement, contrôle et limite des accès, détection et réponse à un incident).

Les nouvelles règles face aux nouveaux risques

Les entreprises ne cèdent pas à la panique. Pour la majorité, des actions ont déjà été initiées pour se conformer à la RGPD. Une interrogation subsiste concernant les contrôles à venir des régulateurs et les éventuelles sanctions. Cela pourrait avoir un impact considérable sur le degré des mesures à mettre en place.

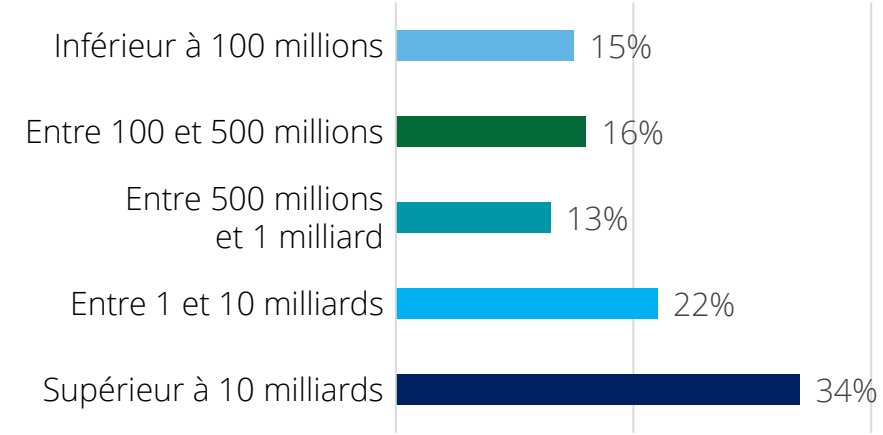
Pourcentage des entreprises ayant initié des actions en lien avec la nouvelle réglementation RGPD



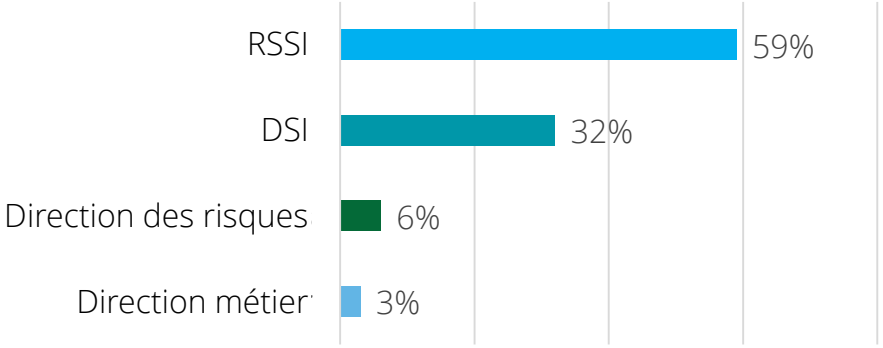
Méthodologie

Réalisée auprès d'un panel de 403 entreprises au cours du deuxième semestre 2017, sur des responsables métiers, IT et Cyber, cette enquête repose sur 20 questions portant sur la maturité de la cybersécurité dans les entreprises.

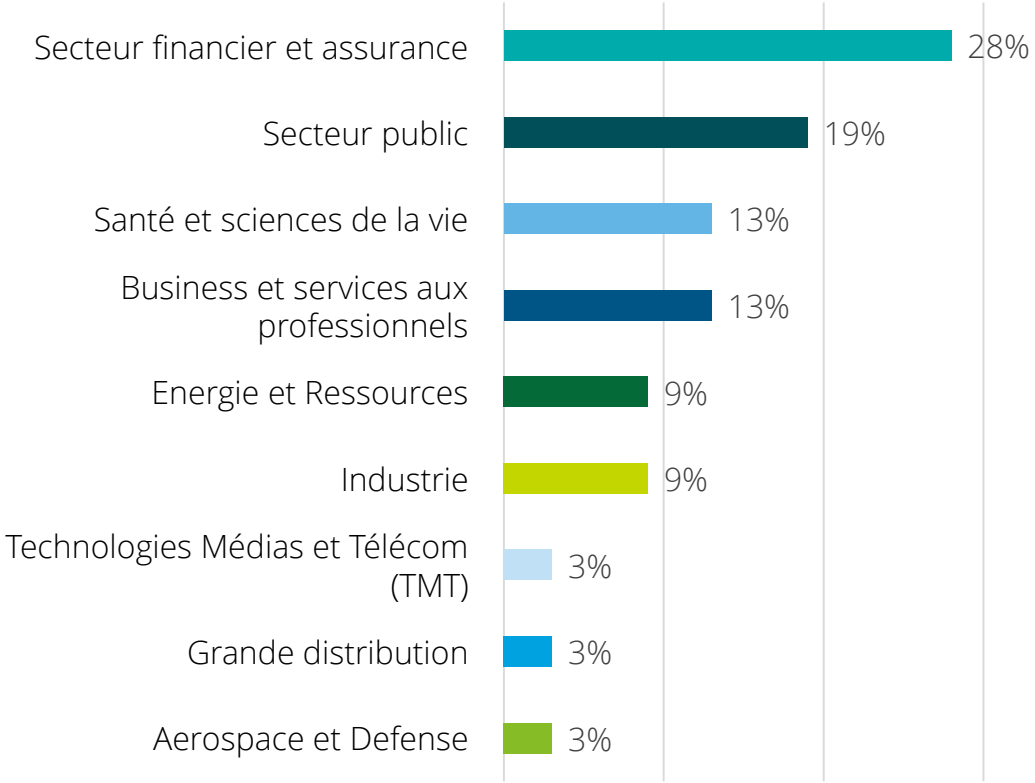
Répartition par chiffre d'affaires



Répartition par fonction



Répartition par secteur d'activité



Auteurs

Michael Bittan
Associé
responsable des activités cybersécurité
Deloitte France

Fouzi Akermi
Manager
activités cybersécurité
Deloitte France

Contacts presse

Relations presse Deloitte

Priscille Holler
+33 (0)1 58 37 93 76
pholler@deloitte.fr

Agence Rumeur Publique

Marie Goislard
+ 33 (0)1 55 74 52 33
marie@rumeurpublique.fr

Deloitte.

A propos de Deloitte

Deloitte fait référence à un ou plusieurs cabinets membres de Deloitte Touche Tohmatsu Limited (DTTL), société de droit anglais (« private company limited by guarantee »), et à son réseau de cabinets membres constitués en entités indépendantes et juridiquement distinctes.
DTTL (ou « Deloitte Global ») ne fournit pas de services à des clients. Pour en savoir plus sur notre réseau global de firmes membres : www.deloitte.com/about. En France, Deloitte SAS est le cabinet membre de Deloitte Touche Tohmatsu Limited, et les services professionnels sont rendus par ses filiales et ses affiliés.

Deloitte fournit des services professionnels en audit & assurance, consulting, financial advisory, risk advisory, juridique & fiscal et expertise comptable à ses clients des secteurs public et privé, quel que soit leur domaine d'activité. Deloitte sert quatre entreprises sur cinq du Fortune Global 500® companies à travers un réseau de firmes membres dans plus de 150 pays, et allie des compétences de niveau international à un service de grande qualité afin d'aider ses clients à répondre à leurs enjeux les plus complexes. Pour en savoir plus sur la manière dont nos 264 000 professionnels make an impact that matters (agissent pour ce qui compte), connectez-vous et échangez avec nous sur Facebook, LinkedIn ou Twitter.

En France, Deloitte mobilise un ensemble de compétences diversifiées pour répondre aux enjeux de ses clients, de toutes tailles et de tous secteurs – des grandes entreprises multinationales aux microentreprises locales, en passant par les ETI et PME. Fort de l'expertise de ses 11 300 collaborateurs et associés, Deloitte en France est un acteur de référence en audit & assurance, consulting, financial advisory, risk advisory, juridique & fiscal et expertise comptable, dans le cadre d'une offre pluridisciplinaire et de principes d'action en phase avec les exigences de notre environnement.

PARTENAIRE OFFICIEL EXPO 2025 GRAND PARIS FRANCE

PARTENAIRE #FRANCE 2023