Les entreprises françaises face aux cyber-attaques

Décembre 2016

Une enquête de Denjean & Associés

en partenariat avec Gan Assurances

CONTEXTE ET MÉTHODOLOGIE DE L'ENQUÊTE

➢ Dans le monde entier, les attaques informatiques se multiplient. Mais dans l'Hexagone, ce fléau explose : l'an dernier, le nombre des cyber-attaques a augmenté de 50% ! *(Source : rapport 2015 de l'Anssi, Agence nationale de sécurité des systèmes d'information)*. Et contrairement à une idée répandue, les principales victimes ne sont pas les grands groupes, mais les PME, qui dans notre pays sont la cible de près de 80% des agressions… *(Source : Syntec)*

➢ Les entreprises françaises sont-elles conscientes des risques qu'elles courent ? De quelles mesures de protection disposent-elles en cette fin d'année 2016 ? Quelle est leur stratégie pour 2017 ?... Denjean & Associés, société d'expertise comptable, d'audit et de conseil, a jugé intéressant de les sonder sur ces thématiques.

➢ Population interrogée : les décideurs d'entreprises en charge de la stratégie informatique.

➢ Denjean & Associés a conçu le questionnaire en partenariat avec Gan Assurances, et a confié la réalisation du sondage à l'institut MRCC.

➢ L'enquête s'est déroulée en ligne, du 7 au 10 novembre 2016.

➢ 200 décideurs ont répondu à l'intégralité des questions, au titre soit de mandataire social (président/ directeur général / gérant…), soit de directeur ou responsable financier, soit de directeur ou responsable informatique / DSI.

➢ A l'issue de l'enquête, Denjean & Associés a analysé les résultats agrégés fournis par MRCC.

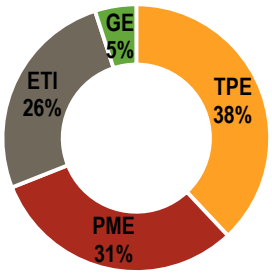
Structure de l'échantillon :

➢ Profil des répondants :

Mandataire social (Président / DG / Gérant…)	32%
Directeur ou Responsable Financier	26%
Directeur ou Responsable Informatique / DSI	42%

➢ Taille des entreprises :

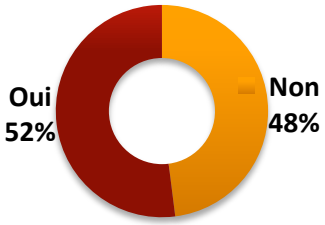
TPE (très petites entreprises) : moins de 2 millions d'euros de CA	38%
PME (petites et moyennes entreprises) : de 2 à 50 millions d'euros de CA	31%
ETI (entreprises de taille intermédiaire) : de 50 millions à 1,5 milliard d'euros de CA	26%
GE (Grandes entreprises) : plus de 1,5 milliard d'euros de CA	5%



RÉSULTATS DE L'ENQUÊTE

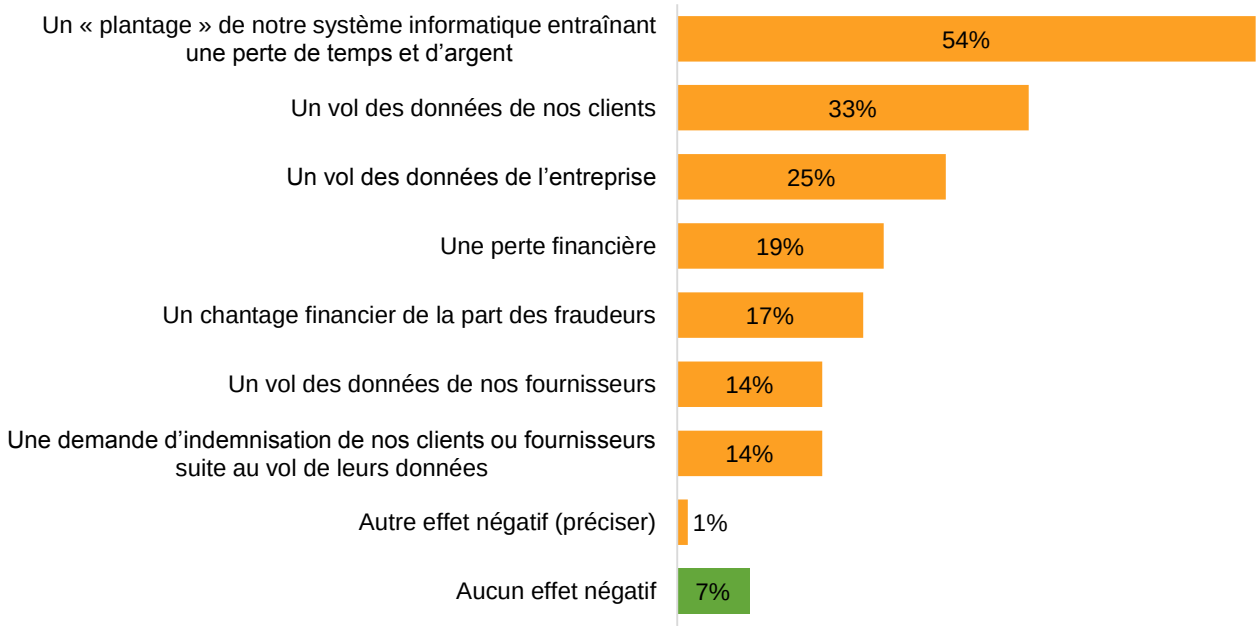
➢ **52% des entreprises ont déjà subi une ou plusieurs tentatives d'attaques visant leur réseau informatique**

Q) Votre entreprise a-t-elle déjà subi une ou des tentatives d'attaques visant son réseau informatique («cyber-attaques»)?
Base : total des répondants



➢ **93% des entreprises ayant déjà vécu des cyberattaques ont pâti de ces agressions**

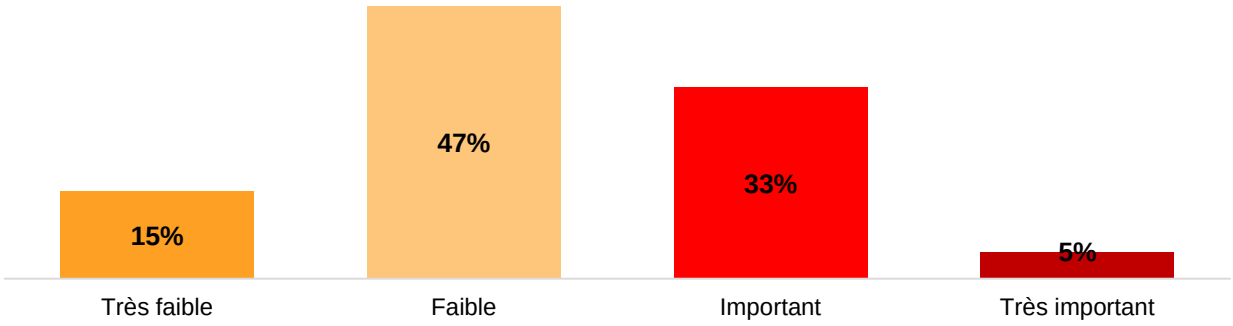
Q) Quels effets négatifs votre société a-t-elle connus du fait des cyber-attaques ?
Base : répondants ayant subi des cyber-attaques



Il est malheureusement exceptionnel qu'une entreprise victime d'un piratage informatique s'en sorte sans dommage. Dans 93% des cas, la société « hackée » subit un ou plusieurs préjudices : arrêt total de son système informatique, vol de données (de l'entreprise / de ses clients / de ses fournisseurs), chantage… Concernant ce dernier point, il est impressionnant de constater que 17% des entreprises piratées ont déjà été victimes d'un "ransomware" (logiciel qui bloque la machine qu'il a infectée et qui exige le paiement d'une rançon pour rendre à l'utilisateur le contrôle de sa machine) !

➢ A l'exception des grands groupes, toutes les entreprises sous-estiment les risques de cyber-attaque

Q) À quel niveau estimez-vous le risque que votre entreprise subisse une cyber-attaque au cours des années à venir ?
Base : total des répondants



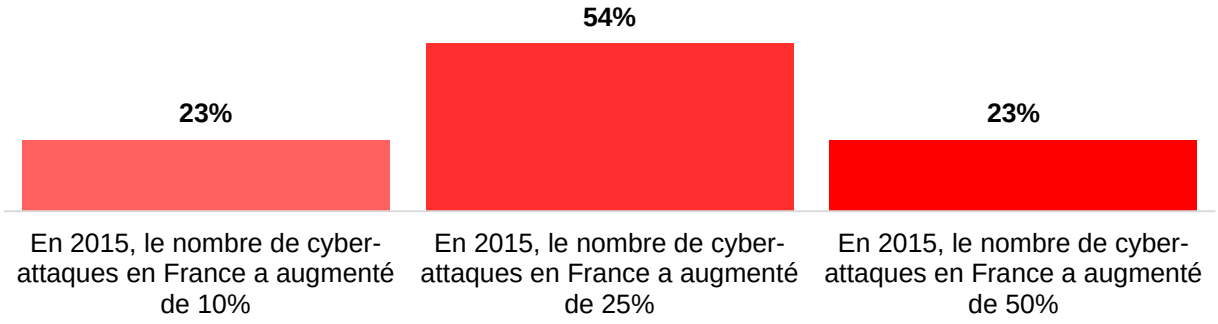
Décomposition des résultats par type d'entreprise :

	"Risque très faible"	"Risque faible"	"Risque important"	"Risque très important"
CA inférieur à 2 millions d'euros (TPE)	25%	58%	17%	0%
CA de 2 à 50 millions d'euros (PME)	11%	45%	34%	10%
CA de 50 millions à 1,5 milliard d'euros (ETI)	8%	38%	48%	6%
CA supérieur à 1,5 milliard d'euros (GE)	0%	11%	89%	0%

Au total, 38% seulement des décideurs considèrent comme "important", ou "très important", le risque que leur société subisse une cyber-attaque ces prochaines années… et ce, alors même que 52% des entreprises ont déjà été victimes d'un piratage informatique ! *« Seuls les décideurs de grandes entreprises apparaissent conscients de la réalité de ce phénomène. A l'autre bout du spectre, les dirigeants de PME sous-estiment fortement les risques liés à la cyber-sécurité* », commente Thierry Denjean, président de Denjean & Associés. Comme nous allons le voir ci-après, cette erreur d'appréciation est notamment due à une méconnaissance de l'ampleur et des cibles de la cyber-fraude dans notre pays…

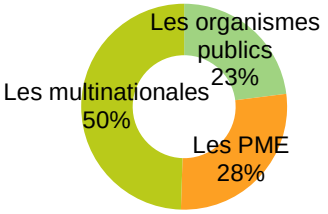
➢ Une méconnaissance de l'ampleur et des cibles du piratage informatique en France

Q) Laquelle de ces trois affirmations est exacte, à votre avis ?
Base : ensemble des répondants



Q) À votre avis, quelle est la cible privilégiée des cyber-attaques en France ?

Base : ensemble des répondants

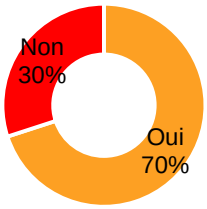


Dans l'ensemble, les décisionnaires d'entreprise se font de fausses idées sur la cyber-fraude. En effet, 77% d'entre eux sous-estiment la vitesse de propagation de ce fléau dans l'Hexagone, pensant que le nombre des cyber-fraudes recensées en France n'a augmenté "que" de 10% ou de 25% l'an dernier, alors qu'il a crû de 50%... Par ailleurs, questionnés sur les cibles visées en priorité par les cyber-fraudeurs, 50% des décideurs citent les multinationales. Tandis que pour 23% des répondants, les organismes publics constituent le premier choix des hackers. Seulement 28% des personnes interrogées connaissent la bonne réponse : ce sont les PME qui concentrent dans notre pays l'immense majorité (environ 80%) des cyber-attaques. *« Les pirates informatiques s'en prennent aux petites structures parce qu'ils savent que beaucoup d'entre elles ont de gros défauts dans la cuirasse qu'il leur sera facile d'exploiter»*, analyseThierry Denjean.

➢ **58% des TPE, environ 75% des PME et des ETI, et 100% des grands groupes se jugent bien protégés contre la cyber-fraude**

Q) Estimez-vous qu'aujourd'hui votre entreprise est bien protégée contre la cyber-fraude ?

Base : ensemble des répondants



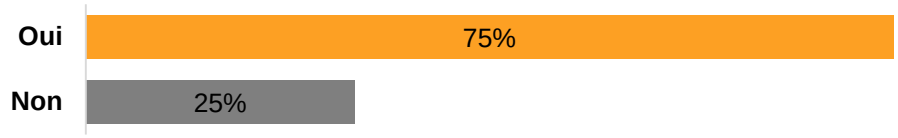
Décomposition des résultats par type d'entreprise :

	Non	Oui
CA inférieur à 2 millions d'euros (TPE)	42%	58%
CA de 2 à 50 millions d'euros (PME)	26%	74%
CA de 50 millions à 1,5 milliard d'euros (ETI)	23%	77%
CA supérieur à 1,5 milliard d'euros (GE)	0%	100%

Globalement, 70% des entreprises s'estiment bien protégées contre la cyber-fraude. Une statistique qui recouvre des disparités : 100% des grands groupes affichent leur confiance dans leurs process de cyber-sécurité, tandis que 58% des TPE et environ 75% des PME et des ETI se jugent bien protégées. Mais de l'avis de Thierry Denjean, les entreprises françaises pèchent par excès d'optimisme : «*Nous avons constaté à quel point les PME, et dans une moindre mesure les ETI, sous-estiment les risques de piratage qu'elles encourent. On peut donc avancer qu'une part significative des structures qui se jugent prêtes à contrer une attaque sont, en réalité, vulnérables…. »*

➢ **75% des sociétés disposent aujourd'hui de process de cyber-sécurité**

Q) Avez-vous déjà mis en place des mesures pour diminuer les risques liés aux cyber-attaques ?
Base : ensemble des répondants



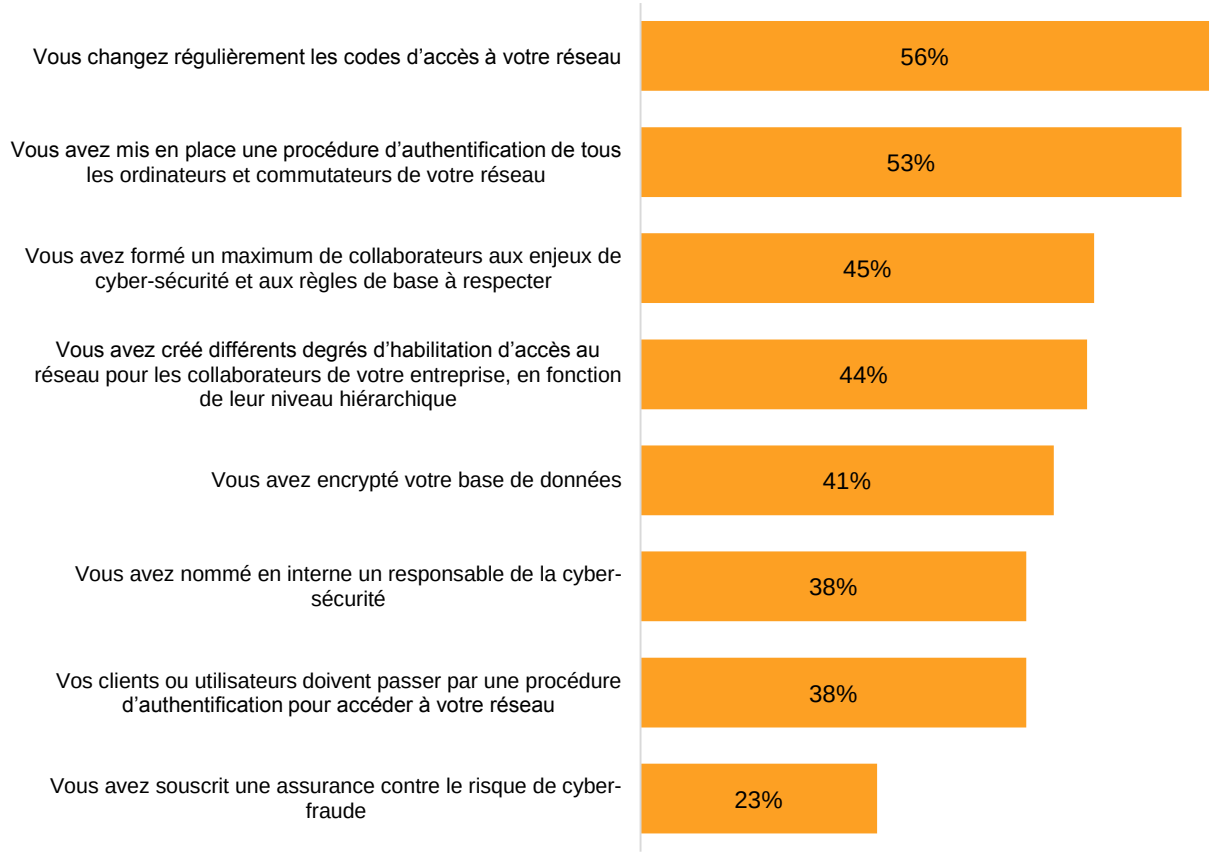
Décomposition des résultats par type d'entreprise :

	Oui	Non
CA inférieur à 2 millions d'euros (TPE)	56%	44%
CA de 2 à 50 millions d'euros (PME)	84%	16%
CA de 50 millions à 1,5 milliard d'euros (ETI)	88%	12%
CA supérieur à 1,5 milliard d'euros (GE)	100%	0%

En cette fin d'année 2016, près d'une TPE française sur deux n'a encore instauré aucune mesure pour diminuer les risques de piratage informatique. A l'inverse, plus de 80% des PME et des ETI (et, sans surprise, 100% des grands groupes) disposent de process de cyber-sécurité.

➢ **Changement régulier des codes d'accès au réseau, procédure d'authentification de tous les ordinateurs et commutateurs : les deux mesures de cyber-sécurité les plus répandues**

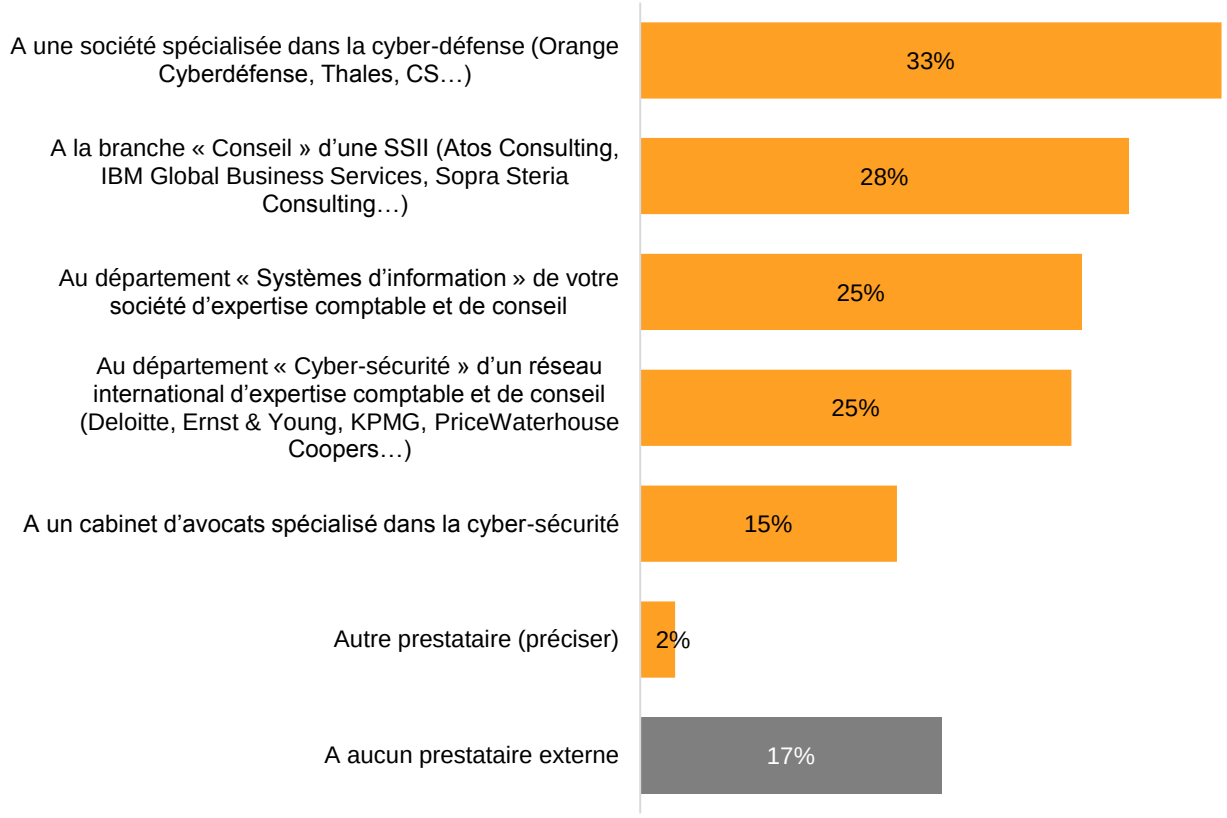
Q) Quelles mesures de cyber-sécurité avez-vous adoptées ?
Base : répondants ayant déjà pris des mesures



Fin 2016, les entreprises ayant adopté une politique de cyber-sécurité ont mis en place, en moyenne, trois mesures. Les plus répandues sont le changement régulier par l'entreprise des codes d'accès à son réseau (mesure existant dans 56% des structures), et l'instauration en son sein d'une procédure d'authentification de tous les ordinateurs et commutateurs (en œuvre dans 53% des entreprises).
La formation interne aux enjeux et aux précautions de base en matière de cyber-sécurité, et la création de différents degrés d'accès au réseau pour les collaborateurs selon leur niveau hiérarchique (respectivement pratiquées par 45% et 44% des sociétés) se disputent la troisième place sur le podium.
Autres mesures-clés, adoptées par environ 40% des entreprises : l'encryptage de la base de données, la nomination d'un responsable de la cyber-sécurité en interne, l'instauration d'une procédure d'authentification pour les clients ou utilisateurs.
Notons enfin que 23% des sociétés ont souscrit une assurance contre le risque de cyber-fraude.

➢ **83% des entreprises qui luttent contre la cyber-fraude se font accompagner par un ou deux prestataires externes**

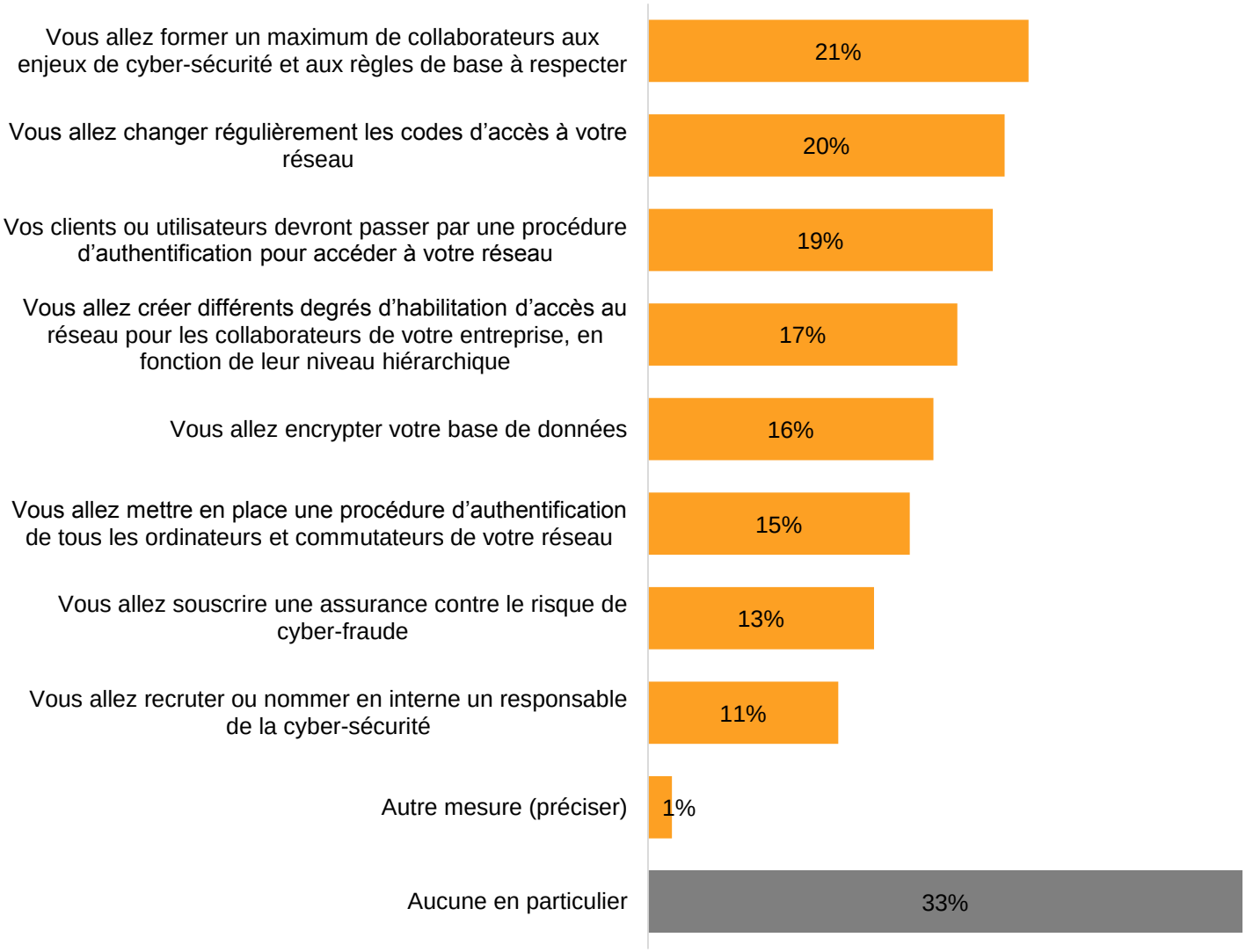
Q) À quel(s) prestataire(s) externe(s) avez-vous fait appel pour vous aider à mettre en place votre stratégie de lutte contre la cyber-fraude ?
Base : répondants ayant déjà mis en place des mesures



Seulement 17% des entreprises qui ont mis en place une stratégie de lutte contre la cyber-fraude ont trouvé toutes les ressources nécessaires en interne. L'immense majorité (83%) a fait appel à un ou deux prestataires externes. Structures expertes en cyber-défense, SSII, sociétés d'expertise comptable et de conseil apparaissent comme les prestataires les plus sollicités.

➢ En 2017, les deux-tiers des entreprises adopteront de nouvelles mesures de cyber-sécurité

Q) Quelles nouvelles mesures de cyber-sécurité pensez-vous adopter en 2017 ?
Base : ensemble des répondants



Au total, 67% des entreprises comptent adopter en 2017 de nouvelles mesures pour lutter contre le piratage informatique.
L'année prochaine, comme le montre le graphique ci-dessus :
- 21% des sociétés formeront pour la première fois leurs salariés aux enjeux et aux règles de base de la cyber-sécurité ;
- 20% des organisations se mettront à changer régulièrement les codes d'accès à leur réseau ;
- 19% des structures instaureront une procédure d'authentification de leurs clients ou utilisateurs ;
- 17% des entreprises créeront différents degrés d'habilitation d'accès au réseau pour leurs collaborateurs, en fonction des niveaux hiérarchiques ;
- 16% des firmes encrypteront leur base de données ;
- 15% des organisations se doteront d'une procédure d'authentification de tous les ordinateurs et commutateurs de leur réseau ;
- 13% des sociétés souscriront leur premier contrat d'assurance contre le risque de cyber-fraude ;
- 11% des entreprises créeront en leur sein un nouveau poste de responsable de la cyber-sécurité.

Par ailleurs, une question ouverte posée aux sociétés ne prévoyant aucune nouvelle mesure de cyber-sécurité en 2017 nous a permis de voir que celles-ci se répartissent en 3 catégories :

1) des sociétés qui s'estiment déjà dotées d'un arsenal de cyber-sécurité suffisant pour leur assurer une bonne protection ;
2) des entreprises qui aimeraient prendre de nouvelles mesures de cyber-sécurité l'an prochain mais qui n'en ont pas les moyens ;
3) des structures se jugeant peu ou pas du tout exposées au risque de cyber-attaque, qui ne voient pas l'intérêt pour elles de prendre des mesures de cyber-sécurité, et qui n'en prendront pas plus en 2017 qu'elles ne l'ont fait jusqu'à présent.

Enfin, en croisant différentes données, on observe que 10% des sociétés n'ayant encore aucun outil de prévention fin 2016 comptent mettre en place une ou plusieurs mesures de cyber-sécurité en 2017. *« Si ces entreprises appliquent leur programme, la proportion des entreprises françaises disposant d'un arsenal plus ou moins étendu de lutte contre le piratage informatique passera de 75% actuellement à 85% fin 2017 »*, se réjouit Thierry Denjean.

➢ 60% des entreprises sont prêtes à consacrer à la lutte contre la cyber-fraude un budget annuel supérieur ou égal à 1% de leur chiffre d'affaires

Q) Quel budget annuel votre entreprise serait-elle prête à consacrer, au total, à une protection efficace contre les risques liés à la cyber-fraude ?
Base : ensemble des répondants

Environ 0,1% de son chiffre d'affaires	11%
Environ 0,5% de son chiffre d'affaires	19%
Environ 1% de son chiffre d'affaires	26%
Environ 1,5% de son chiffre d'affaires	16%
Environ 2% de son chiffre d'affaires	10%
Plus de 2% de son chiffre d'affaires	8%
Aucun budget	10%

Décomposition des résultats par type d'entreprise :

	Aucun budget	Environ 0,1 % du CA	Environ 0,5% du CA	1% du CA ou plus
CA inférieur à 2 millions d'euros (TPE)	23%	19%	17%	38%
CA de 2 à 50 millions d'euros (PME)	0%	2%	23%	76%
CA de 50 millions à 1,5 milliard d'euros (ETI)	0%	8%	17%	75%
CA supérieur à 1,5 milliard d'euros (GE)	0%	33%	22%	44%
Total général	10%	11%	19%	60%

Bonne nouvelle : 90% des entreprises françaises sont disposées à investir chaque année pour se protéger efficacement contre la cyber-fraude, et 60% sont même prêtes à y consacrer un budget supérieur ou égal à 1% de leur chiffre d'affaires. Parmi les différentes catégories d'entreprises, les PME et les ETI se montrent les plus enclines à réaliser un effort financier conséquent: les trois-quarts d'entre elles acceptent de dépenser chaque année pour leur cyber-sécurité entre 1% et 2% de leur chiffre d'affaires.

➢ **Les trois premières réactions des décideurs en cas de cyber-attaque : convoquer une cellule de crise interne, contacter leur prestataire informatique, appeler la police**

Q) En cas de cyber-attaque, quelles seront dans l'ordre vos trois premières réactions ?
Base : ensemble des répondants

	Citations en 1ère position	Citations en 2ème position	Citations en 3ème position	Total citations parmi les 3 réactions prioritaires
Convoquer une cellule de crise interne	**27%**	**15%**	**11%**	**53%**
Contacter votre prestataire informatique externe	**19%**	**21%**	**14%**	**54%**
Appeler la police	**15%**	**14%**	**15%**	**44%**
Téléphoner à vos banquiers	**16%**	**11%**	**8%**	**35%**
Appeler votre assureur	**7%**	**12%**	**14%**	**33%**
Appeler votre expert-comptable	**7%**	**8%**	**7%**	**22%**
Téléphoner à votre avocat	**5%**	**8%**	**11%**	**24%**
Contacter la CNIL	**5%**	**7%**	**11%**	**23%**
Appeler une de vos connaissances qui a déjà subi une cyber-attaque	**1%**	**6%**	**10%**	**17%**
Autre réaction (précisez)	**0%**	**1%**	**1%**	**1%**

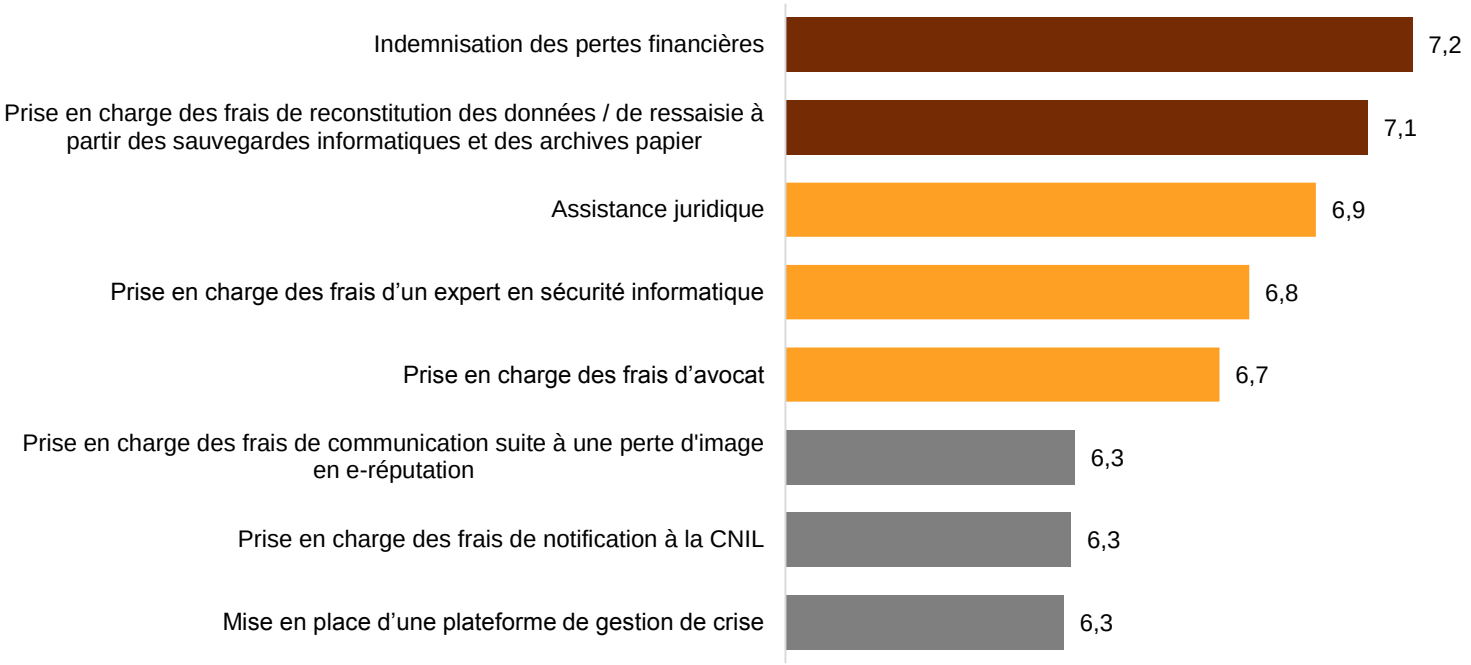
Nous avons demandé aux décideurs d'entreprise de nous dire quelles seraient leurs trois premières réactions s'ils étaient victimes d'une cyber-attaque. Résultats :

- La toute première réaction des décideurs consisterait pour 27% d'entre eux à convoquer une cellule de crise interne, pour 19% à contacter leur prestataire informatique, pour 16% à téléphoner à leurs banquiers, et pour 15% à appeler la police ;
- Au total, en première, deuxième ou troisième urgence, 54% des répondants contacteraient leur prestataire informatique, 53% réuniraient une cellule de crise interne, 44% appelleraient la police, 35% téléphoneraient à leur banquier, et 33% contacteraient leur assureur.

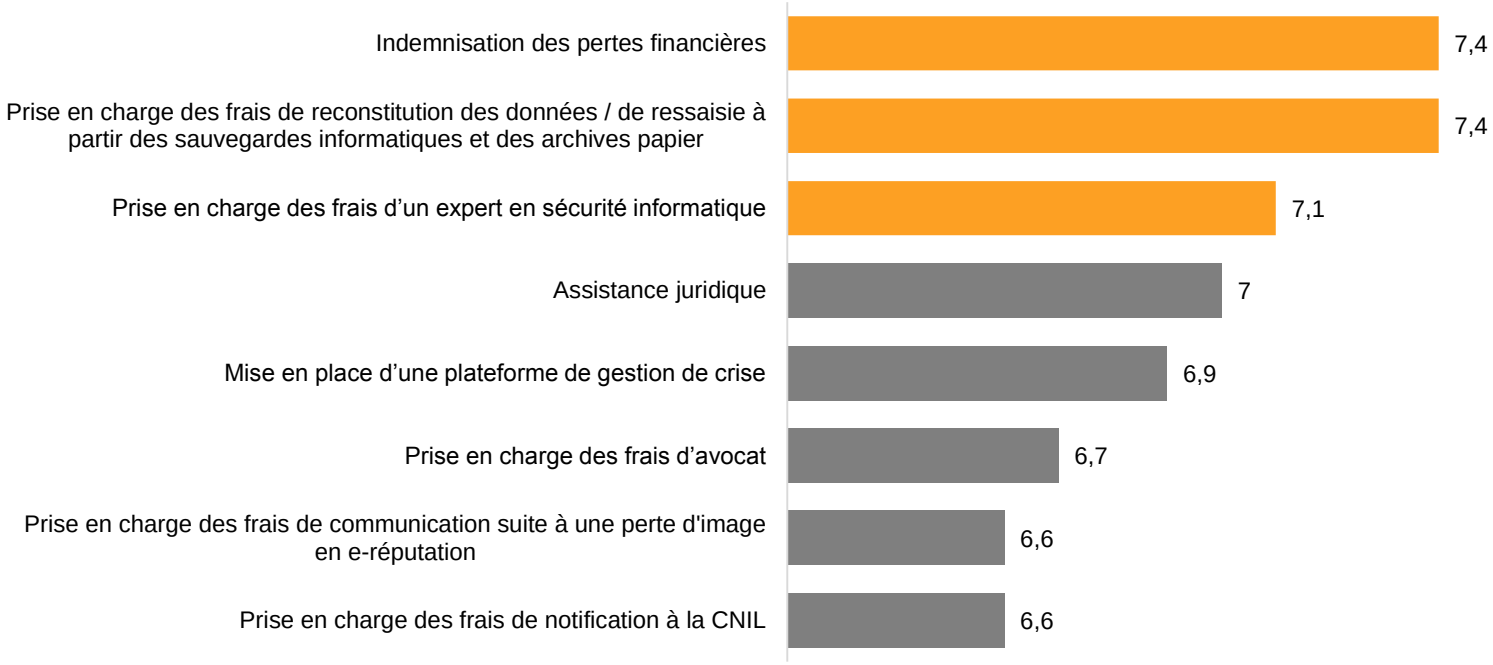
Dans les faits, quel est le premier réflexe que doivent avoir des dirigeants d'entreprise face à une cyber-attaque ? « Effectuer un constat technique » indique la Police Nationale, dans un document intitulé "*Réagir à une attaque informatique : 10 préconisations*". A cet effet, la Police Nationale recommande aux décideurs l'une ou l'autre des démarches suivantes, selon leur préférence : contacter le service de police ou de gendarmerie le plus proche pour faire intervenir un expert en cyber-criminalité ; ou procéder eux-mêmes au constat technique (ce qui suppose que l'entreprise soit dotée d'un service informatique) ; ou faire réaliser ce constat par un prestataire informatique externe.

➢ **Indemnisation des pertes financières, prise en charge des frais de reconstitution/ ressaisie des données, assistance juridique, prise en charge des frais d'un expert en sécurité informatique : quatre garanties assurantielles jugées utiles**

Q) Certains assureurs proposent des garanties visant à protéger les entreprises victimes de cyber-attaques. Veuillez noter les garanties ci-dessous de 0 à 10 selon leur utilité en cas de cyber-attaque dans votre société.
Base : ensemble des répondants



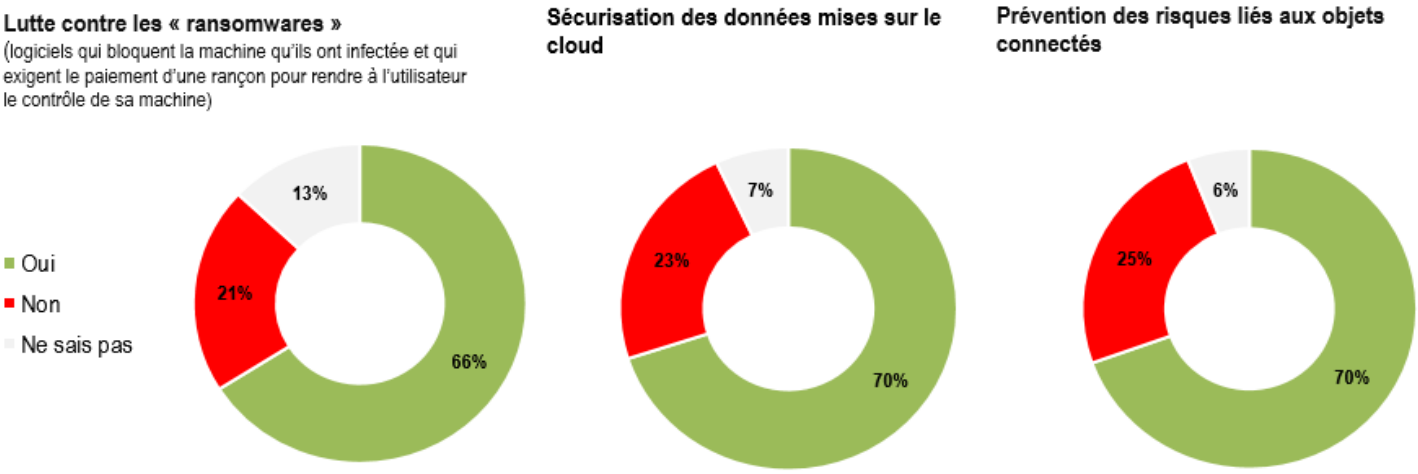
Notes attribuées aux différentes garanties par les décideurs ayant déjà subi des cyber-attaques :



Qu'ils aient déjà vécu une cyber-attaque ou non, les répondants jugent que les garanties les plus utiles que peut proposer un assureur sont l'indemnisation des pertes financières, la prise en charge des frais de reconstitution/ ressaisie des données, l'assistance juridique et la prise en charge des frais d'un expert en sécurité informatique.
Dans l'ensemble, les décideurs d'entreprise s'accordent sur la hiérarchie des garanties assurantielles. A une exception près toutefois, qui concerne la mise en place d'une plateforme de gestion de crise : les décideurs n'ayant jamais affronté de cyber-attaque s'intéressent peu à cette garantie, lui attribuant la médiocre note de 5,7/10… tandis que les décideurs ayant déjà vécu un piratage informatique la jugent d'une réelle utilité, attestée par une note de 6,9/10.

➢ Des décideurs d'entreprise conscients des nouveaux risques et prêts à agir !

Q) Au cours des trois prochaines années, allez-vous vous préoccuper des sujets suivants ?
Base : ensemble des répondants



« Si l'on exclut les dirigeants de très petites structures, peu ou pas du tout concernés par ces sujets, les décideurs apparaissent bien conscients des nouveaux risques encourus par les entreprises, et décidés à les combattre », souligne Thierry Denjean.
En effet, 66% des décisionnaires indiquent qu'ils se préoccuperont au cours des trois années à venir de lutter contre les "ransomwares" ; 70% disent qu'ils s'attacheront à sécuriser les données mises sur le "cloud" ; et 70% déclarent qu'ils veilleront à prévenir les risques liés aux objets connectés…
Et si, au-delà des grandes entreprises, les ETI et même les PME françaises étaient en train de s'ouvrir aux réalités des cyber-risques ?