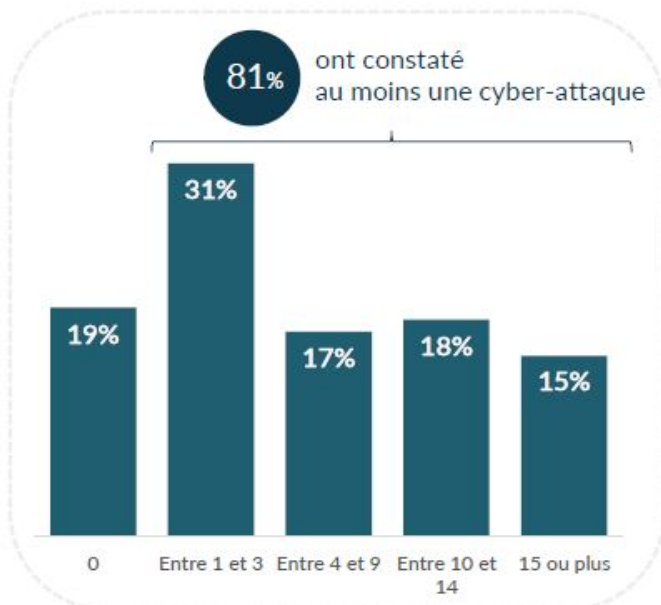


# Cybersécurité : un RSSI sur deux voit son budget augmenter en 2016

Les RSSI ne sont plus les faire-valoir d'une stratégie de cyber-sécurité que dédaignent les directions générales. Selon un sondage d'OpinionWay pour le Cesin (une association de responsables de la sécurité des SI), 88 % des RSSI pensent désormais que la question de la sécurité des SI est jugée importante par leur direction générale. Presque au même niveau que le digital, que les RSSI voient comme un sujet stratégique pour leur organisation dans 93 % des cas. L'étude ne s'étend toutefois pas sur les frictions potentielles entre ces deux stratégies, la transformation numérique réclamant souvent le déploiement rapide d'applicatifs, une exigence potentiellement génératrice de nouveaux risques.

Q5. Combien de cyber-attaques ont été constatées dans votre entreprise au cours des 12 derniers mois ?



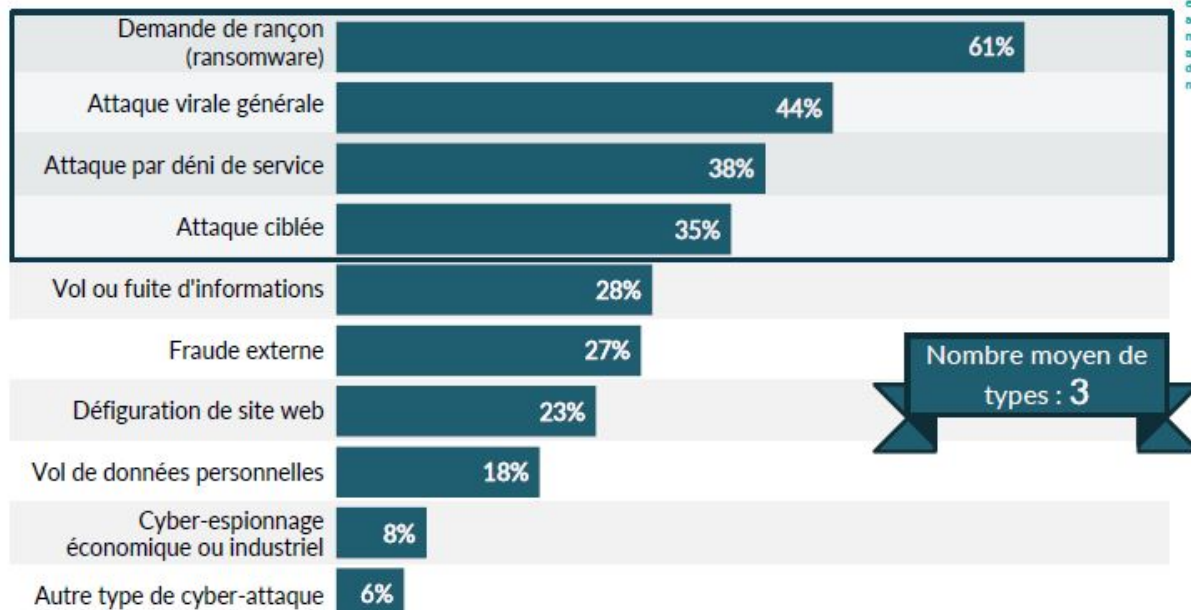
Nombre moyen d'attaques : 13

Nombre d'ordinateurs	Base	Nb moyen
Moins de 999 ordinateurs	22*	2,2
Entre 1 000 et 9 999 ordinateurs	51*	7,3
Entre 10 000 et 49 999 ordinateurs	26*	14,3
50 000 ordinateurs ou plus	26*	32,1

Si les directions générales ne nient plus l'importance de la sécurité, c'est qu'elles peuvent difficilement ignorer l'impact des cyberattaques sur les entreprises. Les très médiatisées affaires Sony Pictures, Target ou Ashley Madison sont passées par là. Et les cyberattaques sont devenues une réalité de leur organisation. Presque du business as usual. Selon les 125 RSSI interrogés par OpinionWay, une organisation française a subi en moyenne 13 attaques au cours des 12 derniers mois. Ce chiffre enflé pour les très grandes entreprises et atteint 32 assauts par an dans les organisations comptant plus de 50 000 postes de travail.

Q6. Quel(s) type(s) de cyber-attaque votre entreprise a-t-elle constaté(s) au cours des 12 derniers mois ?

102  
entreprises  
ayant constaté au  
moins une cyber-  
attaque au cours  
des 12 derniers  
mois

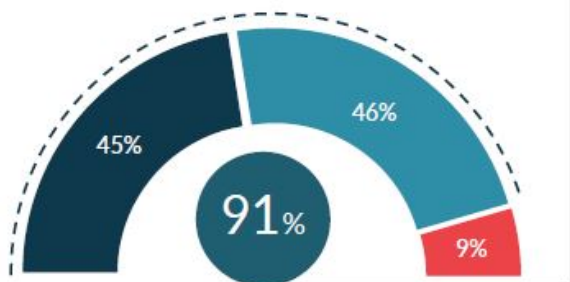


## Ransomware : la star de 2015

Les RSSI se préoccupent avant tout des conséquences d'un vol ou d'une fuite d'informations, d'un vol de données personnelles, d'une attaque virale généralisée ou des attaques ciblées. La réalité des assauts vécus par les organisations est toutefois sensiblement différente : ce sont avant tout les ransomwares (malwares chiffrant les données et réclamant une rançon) qui se sont propagés ces 12 derniers mois. Cette forme de cybercrime, rencontrée au cours de 2015 par plus de 61 % des RSSI, devance les attaques virales se propageant sur le réseau et les dénis de service (DDoS). Les attaques ciblant l'organisation en particulier, les vols ou fuites de données et les vols de données personnelles n'arrivent que bien après. Mais, étant donné leurs conséquences médiatiques, économiques et sur l'image des organisations, il est logique que les RSSI redoutent plus ces formes d'attaque que des menaces plus répandues, mais jugées moins pernicieuses. Encore que la récente mésaventure du ministère des Transports avec un ransomware soit de nature à faire réfléchir.

Si les RSSI ont le sentiment d'avoir l'appui de leur direction, ils aimeraient voir cette prise de conscience se traduire plus rapidement en moyens supplémentaires – techniques, budgétaires et surtout humains. 64 % d'entre eux jugent les budgets consacrés au sujet insuffisants ou très insuffisants. Toutefois, la tendance est clairement au coup de pouce budgétaire sur le sujet, près d'un RSSI sur deux expliquant que son organisation va augmenter le budget cybersécurité en 2016. Et 65 % d'entre eux se disent confiants quant à la capacité de leur entreprise à prendre en compte les enjeux liés aux réalités de la sécurité IT.

Q16. Votre entreprise a-t-elle mis en place des limitations sur les usages des salariés (du type limitation d'usage de sites d'échanges de données, filtrage web, restrictions sur l'utilisation de périphériques...)?

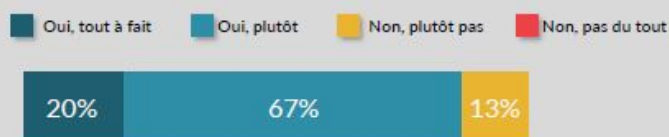


91%  
ont mis en place des limitations sur les usages des salariés

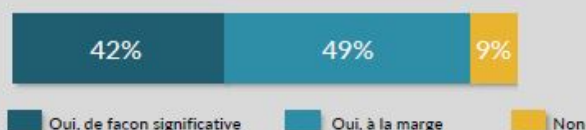
- Oui, ces limitations ont été mises en place
- Oui, mais seulement certaines limitations ont été mises en place
- Non, aucune limitation n'a été mise en place

116 entreprises ayant mis en place des contraintes

Q17. Ces contraintes sont-elles acceptées par les salariés ?



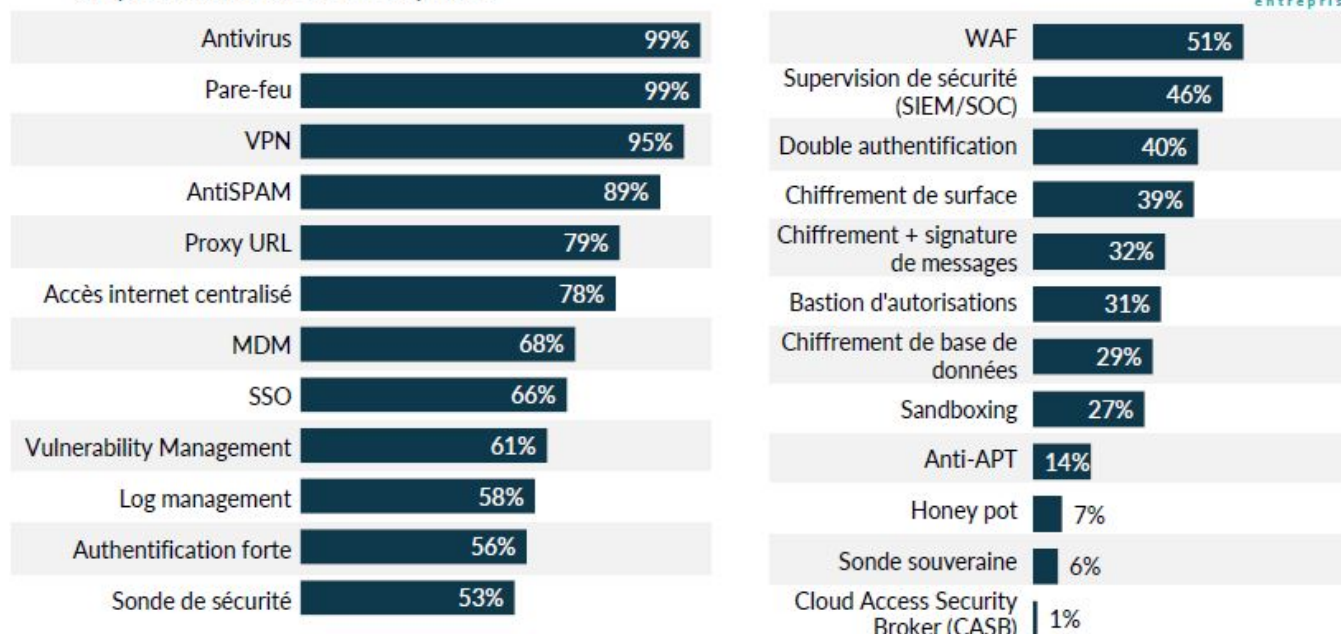
Q18. Et, globalement, la mise en place de ces limitations a-t-elle eu un impact concret sur la cyber-sécurité de votre entreprise ?



## Nouveaux usages, vieilles solutions

Pour les décideurs interrogés, ces enjeux sont d'abord organisationnels. Le premier d'entre eux concerne la gouvernance de la cybersécurité : pour s'intégrer à la stratégie de l'entreprise, celle-ci a besoin d'un sponsor de haut niveau. S'y ajoutent la formation et la sensibilisation des utilisateurs. Dans près de 6 entreprises sur 10, des actions de sensibilisation aux cyber-risques sont menées auprès des utilisateurs. Mais 48 % des RSSI estiment encore que ces derniers ne respectent pas les recommandations formulées. Et ce même si les limitations d'usage qui sont imposées aux salariés dans plus de 9 entreprises sur 10 sont plutôt bien acceptées selon les RSSI et produisent leurs fruits.

Q8. Parmi les solutions de protection suivantes, quelles sont celles qui ont été mises en place dans votre entreprise ?



Au-delà de ces enjeux, 58 % des décideurs interrogés s'inquiètent du décalage entre les solutions

de protection existantes et les nouveaux usages du numérique (le BYOD, les objets connectés, le Cloud). De facto, les solutions de protection majoritairement déployées restent des plus traditionnelles (avec le trio antivirus, pare-feu et VPN). Et des technologies plus nouvelles, comme les solutions anti-APT ou les gestionnaires d'authentification dans le Cloud (Cloud Access Security Broker), sont, elles, bien plus marginales. Le tout alors que ces usages nouveaux connaissent un développement galopant. 85 % des RSSI admettent ainsi que leur entreprise stocke des données dans le Cloud, en majorité sur des infrastructures publiques ou hybrides.

**A lire aussi :**

[Alain Bouillé, Cesin : « sans sécurité, la transformation numérique est un non-sens »](#)

[Les RSSI ont-ils réussi à dompter leur budget ?](#)

**Crédit photo : Sergey Nivens / shutterstock**