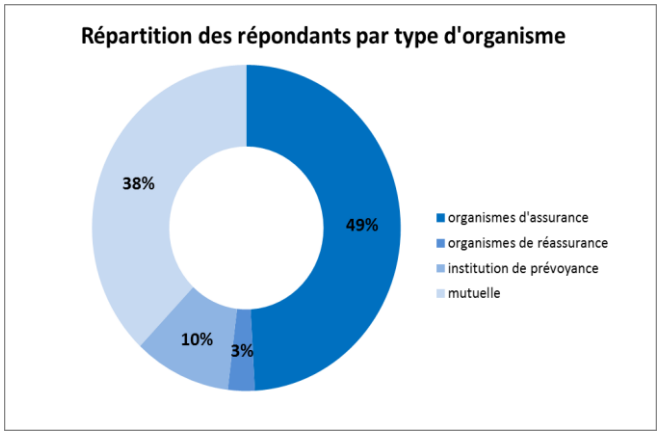
**Note de synthèse concernant l'enquête ACPR de 2017 portant sur la cyber-sécurité**

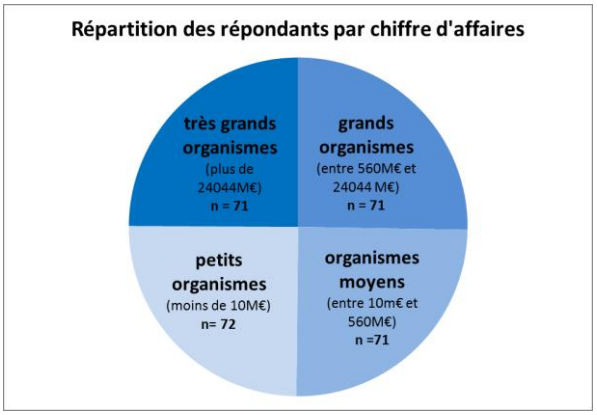
Dans la continuité de l'enquête de 2016 relative à la qualité des données, au système d'information (SI) et à la sécurité du système d'information (SSI), le SGACPR a lancé au quatrième trimestre 2017 une enquête portant sur la gestion de la sécurité du système d'information.

285 organismes ont répondu à cette nouvelle enquête. Ils représentent environ 83% du chiffre d'affaires total du marché de l'assurance et de la réassurance français.

Les 140 organismes d'assurance les plus importants (49% des répondants dont les 20 premiers groupes d'assurance français) représentent à eux seuls 70% du chiffre d'affaires total des organismes ayant répondu.



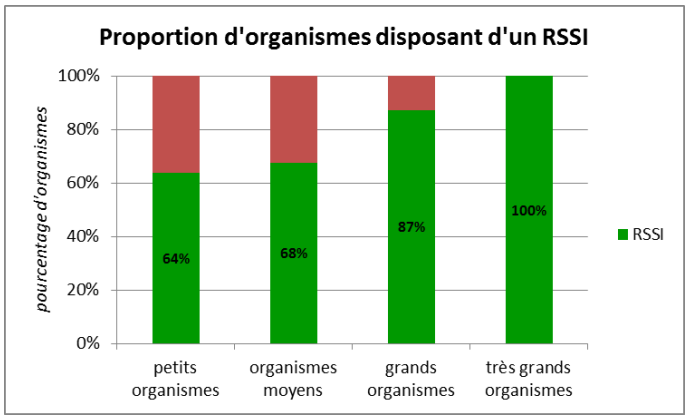

Pour analyser les réponses, les répondants ont été répartis dans des quartiles selon le montant du chiffre d'affaires.



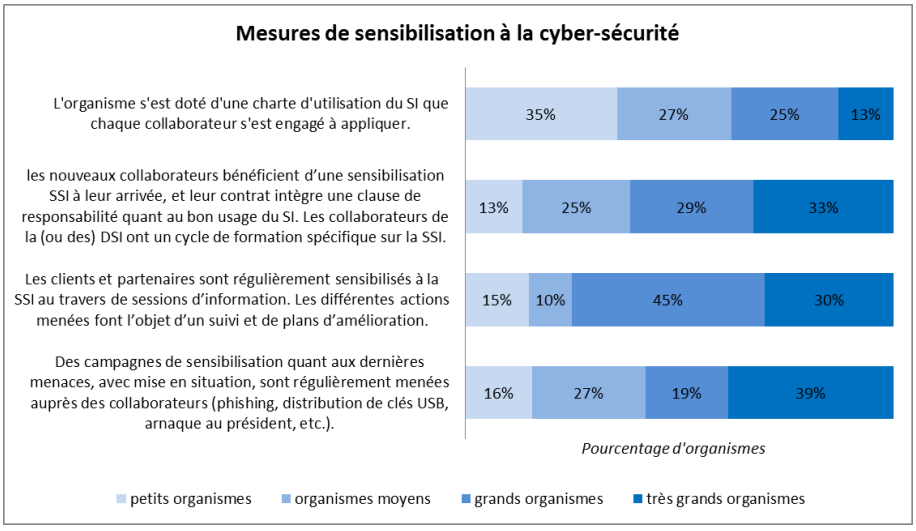
## Un niveau inégal de maturité de la gouvernance de la sécurité du SI

Le niveau de maturité, estimé par les organismes, de la gouvernance de la sécurité de leur SI est très différent suivant leur taille. Ainsi, les fonctions de direction sont davantage associées aux décisions en matière de cyber-sécurité chez les plus grands organismes (64%) que chez les plus petits (28%). Chez ces derniers, la cyber-sécurité est encore gérée très majoritairement par les équipes de production système et réseau, ou par un prestataire externe intervenant pour leur compte.

Par rapport à l'enquête de 2016, la proportion d'organismes qui disposent d'un responsable de la sécurité du SI (RSSI) reste inchangée (80%), avec un écart encore marqué entre petits et grands organismes.




Dans l'ensemble, les organismes mobilisent encore trop peu de moyens pour sensibiliser leurs utilisateurs ou leurs partenaires à la cyber-sécurité : 44% d'entre eux ne se contentent que de la signature d'une charte d'utilisation du SI, sans formations ou campagnes de sensibilisation spécifiques à la cyber-sécurité. Pour les petits organismes, cette proportion s'élève à 62%.



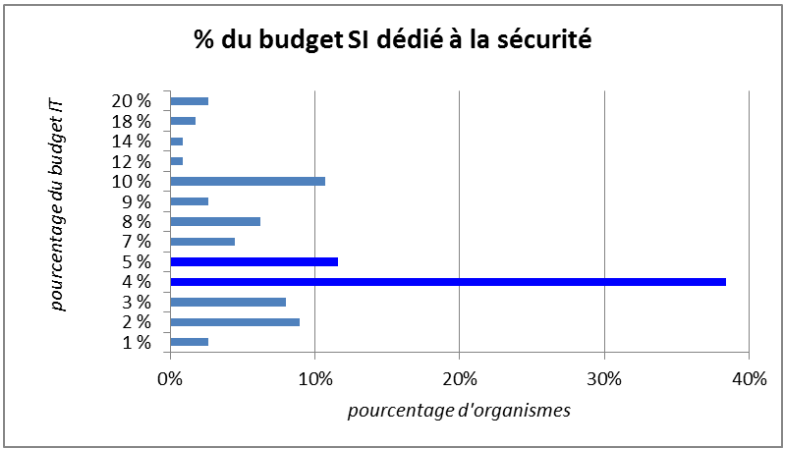

Par ailleurs, seuls 32% des organismes intègrent la sécurité du SI comme critère de sélection de leurs prestataires externes.

**Des coûts relatifs à la sécurité du SI difficile à estimer**

L'enquête révèle aussi que les organismes peinent à évaluer les coûts liés à la sécurité du SI et donc à définir un budget dédié. Ainsi, 27% des organismes n'attribuent pas de budget spécifique à la sécurité du SI, et les deux tiers ne peuvent évaluer précisément tous les postes de coûts liés à la sécurité du SI malgré un budget consacré. Enfin, 15% des organismes disposant d'un budget dédié n'ont pas répondu à la question quantitative relative au pourcentage de budget SI dédié à la sécurité.

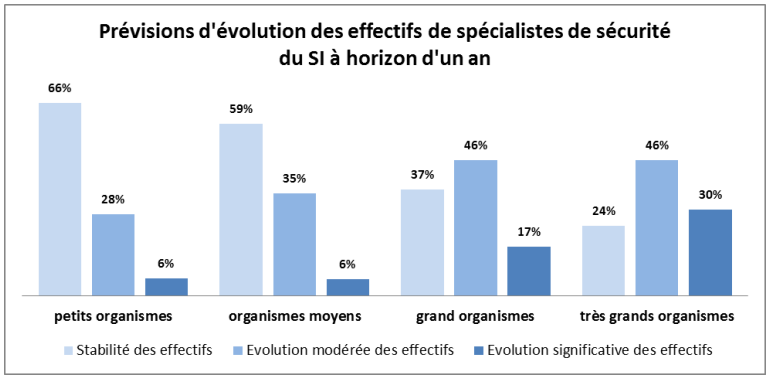
Le pourcentage moyen du budget SI dédié à la sécurité se situe entre 4% et 5% (50% des réponses) avec :

- 20% des répondants donnant une réponse comprise entre 1% et 3% ;
- 30% des répondants donnant une réponse entre 5% et 20%;



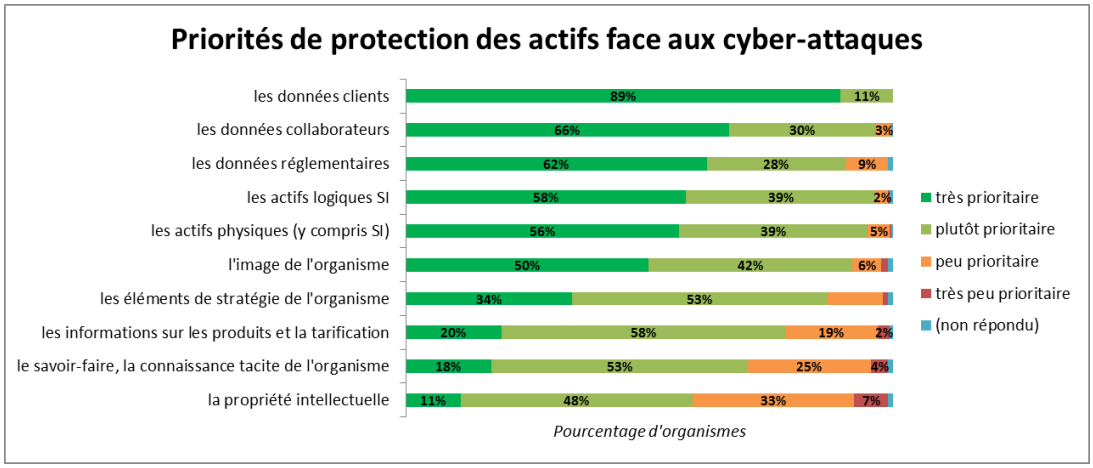

29% des organismes n'identifient jamais dans leurs projets SI la part du budget liée à la sécurité et un peu plus de la moitié d'entre eux ne la définissent que pour les projets SI considérés comme majeurs.

Enfin, malgré la prise de conscience des risques inhérents aux cyber-attaques, on note que 46% des organismes n'envisagent pas de faire évoluer leurs effectifs de spécialistes en sécurité SI à horizon d'un an. On remarque par ailleurs que l'évolution de ces effectifs est positivement corrélée à la taille de l'organisme.



**Une connaissance du SI encore insuffisante pour protéger les actifs les plus sensibles de l'organisme**

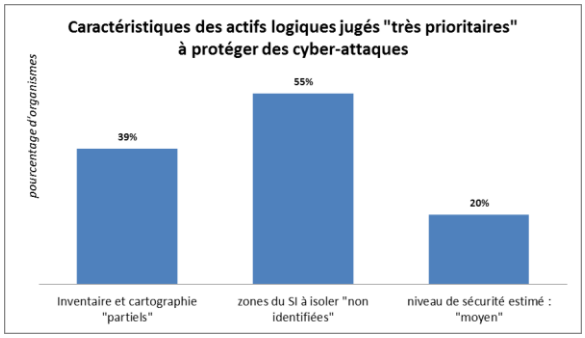
S'agissant des actifs à protéger prioritairement des cyber-attaques, les données clients arrivent très nettement en tête pour 89% des organismes. Viennent ensuite à égalité les données réglementaires, les données collaborateurs et les actifs logiques (applicatifs, processus, documentation,…) et physiques (postes informatiques, serveurs, réseaux, téléphonie,…) du SI.




On remarque aussi que l'intégration de la nouvelle réglementation RGPD (Règlement Général sur la Protection des Données) à la politique globale de sécurité du SI (PGSSI) n'est citée que par 23% des organismes. Seuls les très grands organismes semblent avoir commencé à intégrer cette nouvelle réglementation à leur problématique de sécurité des données. Cette situation devrait néanmoins rapidement évoluer avec, d'une part la mise en place effective de cette réglementation à partir de mai 2018, et d'autre part, la volonté des organismes de protéger de façon prioritaire leurs données clients des cyber-attaques.

Les réponses des organismes qui considèrent leurs actifs logiques comme « très prioritaires » à protéger des cyber-attaques, montrent que ceux-ci n'ont pas toujours une connaissance assez approfondie de leur SI, et dans une proportion non négligeable, un niveau de sécurité suffisant ; en effet :

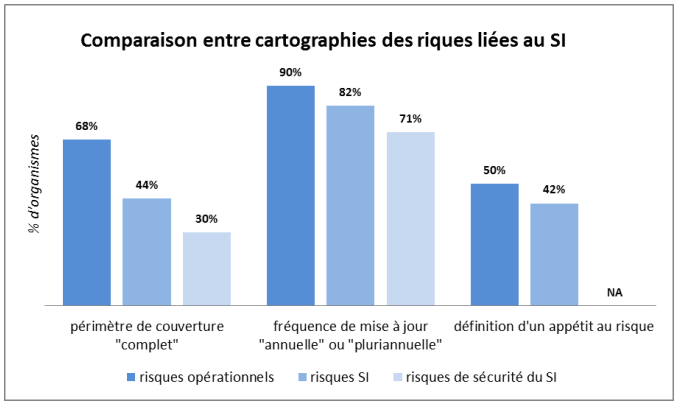
- l'inventaire et la cartographie des SI sont encore « partiels » pour respectivement 39% des organismes.
- plus de la moitié de ces derniers ne peuvent pas identifier les zones du SI à isoler en cas de cyber-attaque.
- 20% des organismes considèrent que le niveau de sécurité de leurs actifs logiques est « moyen », soit une proportion plus élevée que ceux qui l'estiment comme « très bon » (9%).



Enfin, 37% des organismes n'ont qu'une connaissance partielle des versions de leurs actifs, et 32% ne disposent pas de politique contraignante de gestion des versions. À noter que lorsqu'une telle politique existe, le suivi des versions est amélioré.

**La cartographie des risques de sécurité du SI n'est pas aussi aboutie que celle des risques opérationnels ou des autres risques affectant le SI**

La comparaison des caractéristiques de ces trois cartographies des risques montre que les risques de sécurité du SI sont moins bien identifiés et évalués que les deux autres pour lesquels les organismes ont investis depuis plus longtemps.




Concernant plus précisément la cartographie des risques de sécurité du SI :

- les deux tiers des organismes ne disposent pas du périmètre complet de cette cartographie, et 11% déclarent même ne pas en avoir.
- 29% des organismes ne mettent pas à jour au moins annuellement cette cartographie alors que les menaces sont en constante évolution et que les moyens de s'en protéger évoluent aussi rapidement. Seuls 12% des organismes révisent de façon « pluriannuelle » cette cartographie (contre 18% pour les cartographies des risques opérationnels et des risques SI).
- la responsabilité finale des risques de sécurité du SI est largement partagée au sein de l'organisme, quelle que soit sa taille, alors que le directeur des risques est souvent le seul responsable de la cartographie des risques opérationnels et le DSI le seul responsable des risques SI.

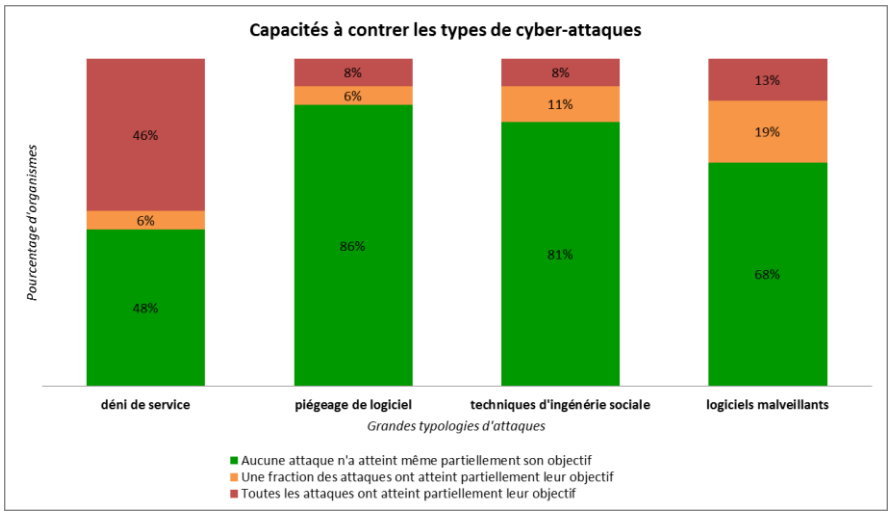
**La nature et le nombre d'attaques subies restent encore très difficiles à évaluer par les organismes**

Comparé à l'enquête réalisée en 2016, le pourcentage d'organismes qui ne disposent pas d'une typologie de cyber-attaques susceptibles de les menacer n'a pas évolué (34%).

Plusieurs réponses à l'enquête relatives aux cyber-attaques illustrent la difficulté que rencontrent les organismes pour recenser et comptabiliser les cyber-attaques affectant leur SI. La très grande variabilité du nombre d'attaques déclarées montre qu'il n'existe pas encore de consensus entre les organismes pour établir une définition et des critères communs caractérisant une cyber-attaque. Les réponses permettent néanmoins de relever les points suivants :

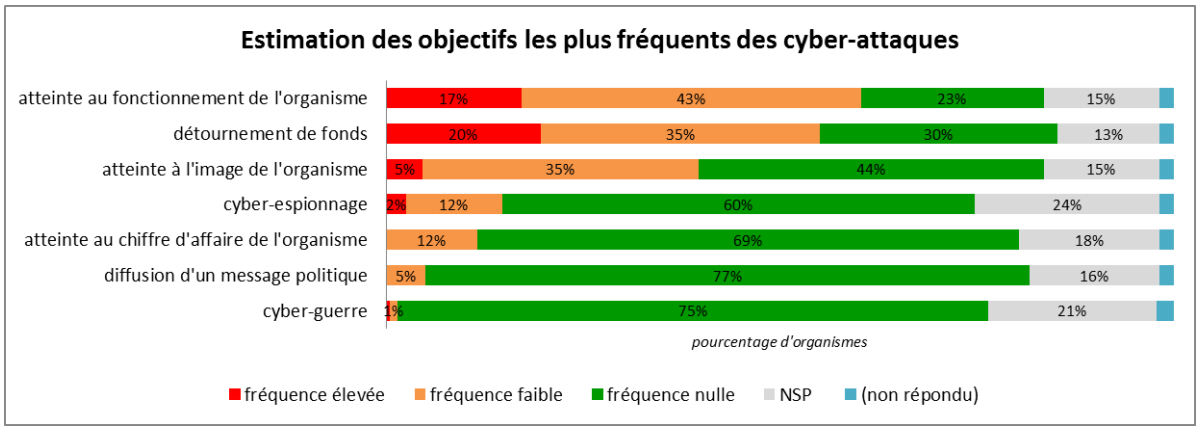
- 10% des répondants ne recensent pas les cyber-attaques affectant leur SI.
- Parmi ceux qui déclarent recenser les cyber-attaques, 14% d'entre eux n'ont pas répondu à la question concernant la quantification, par grande typologie, du nombre de cyber-attaques ciblant leur organisme (attaques totales *vs* attaques non-contrées).
- 9% des organismes déclarent n'avoir subi aucune attaque durant l'année passée, ce qui parait peu probable.

Le ratio nombre d'attaques non contrées sur nombre d'attaques globales déclarées, pour chacun des grand types d'attaques, fait apparaître que les attaques de type "déni de service" sont considérées comme les plus difficiles à contrer (54% des organismes qui déclarent subir des attaques de déni de service ne parviennent pas à les contrer totalement).

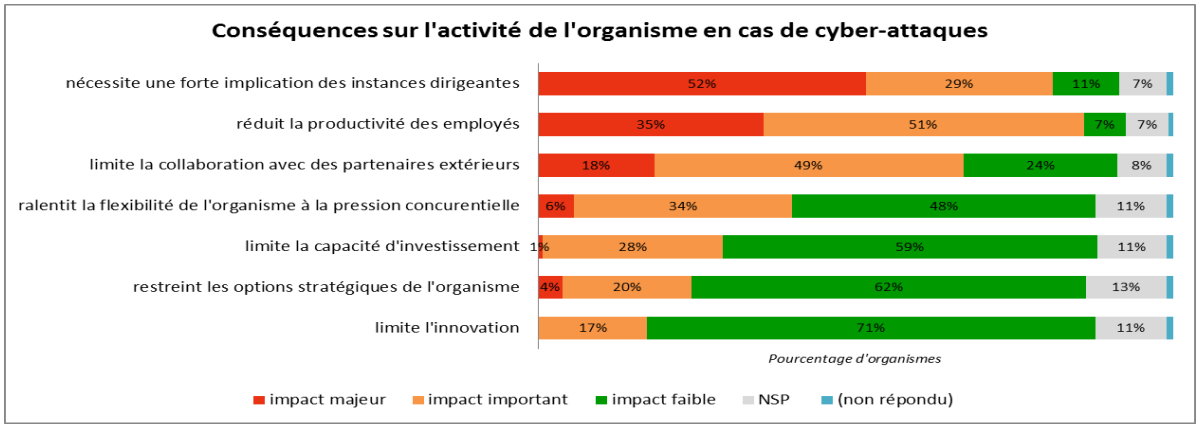


## Estimation des objectifs recherchés et des conséquences en cas de cyber-attaques

Les atteintes au bon fonctionnement de l'organisme et les tentatives de détournement de fonds sont les deux objectifs de cyber-attaques les plus fréquemment cités.

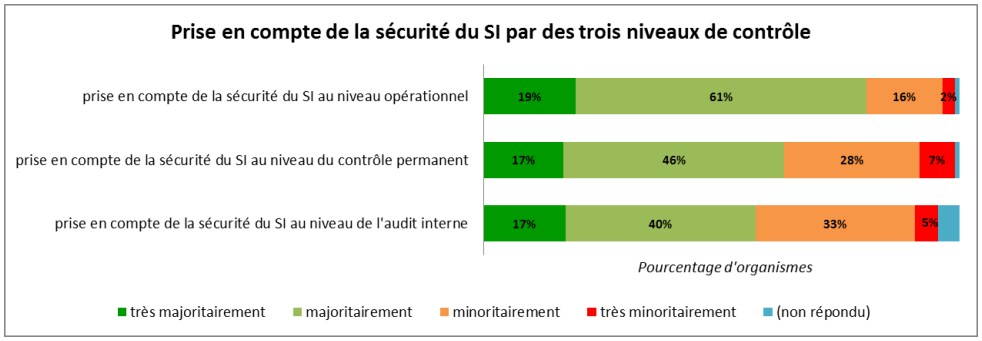



Plus de la moitié des organismes mentionnent la forte implication des instances dirigeantes comme principale conséquence d'une cyber-attaque, avant la réduction de la productivité des employés.




## Les trois niveaux de contrôle constituent aussi une protection pour se prémunir des effets des cyber-attaques

Il ressort de l'enquête que le niveau opérationnel est le niveau de contrôle le plus impliqué sur la problématique de sécurité du SI par rapport au contrôle permanent et à l'audit interne.



La comparaison des résultats de la présente enquête avec ceux de l'enquête de 2016 souligne une amélioration de la fréquence de contrôle de l'audit interne : 19% des organismes réalisent des audits au moins annuellement, contre seulement 13% en 2016.

Les équipes d'audit interne ont plus fréquemment recours à des prestations extérieures (77%), qu'à des renforts ponctuels de leurs équipes opérationnelles (11%). Par ailleurs, 46% des organismes déclarent disposer de compétences en sécurité du SI au sein de leurs équipes.

## Les principales mesures opérationnelles existantes pour réduire le risque de cyber-attaques, ne sont pas encore pleinement exploitées au sein des organismes

### Tests de vulnérabilité

Les applications critiques sont majoritairement testées tous les ans, ou par période de 3 ans pour environ les trois quarts des organismes.
Les autres organismes n'identifient pas d'applications critiques (7%) ou ne réalisent des tests que de manière irrégulière (19%).

### Revues des habilitations applicatives

Le processus de gestion des habilitations est bien mis en place dans les organismes, mais une proportion importante d'entre eux ne révise pas encore au moins annuellement les habilitations :

- 34% des organismes au regard des activités opérationnelles ;
- 24% des organismes par synchronisation avec les processus RH (mouvements de personnel).

A l'opposé, 20% des organismes effectuent une révision trimestrielle de celles-ci.

### Méthodologie de projet

La sensibilisation à la sécurité du SI, via une méthodologie projet spécifique, est intégrée par les trois quarts des organismes, mais sa mise en œuvre est peu contraignante.
Ainsi, lors de la réalisation d'un projet SI :

- 75% des organismes réalisent les recettes sans y inclure de cas de tests de sécurité du SI.
- 78% des organismes ne réalisent pas de tests d'intrusion systématiques avant la mise en production.

## Les organismes sous-évaluent l'intérêt de disposer d'un plan de gestion de crise opérationnel et régulièrement testé

Environ 10% des organismes déclarent ne disposer d'aucun plan de gestion de crise documenté et régulièrement revu pour faire face à une cyber-attaque, alors que celui-ci est pourtant essentiel pour gérer la crise (ex : communication externe), et le cas échéant, pour piloter les plans de continuité métiers et SI.
De plus, parmi ceux qui déclarent en disposer, 46% ne l'ont jamais testé en situation réelle.