TOLÉRANCE AU CHANGEMENT

Un dernier facteur à prendre en compte pour comprendre dans quelle mesure les entreprises doivent accepter de nager au milieu des requins, est leur capacité à gérer le changement informatique. Comme nous l'avons souligné plus haut, les approches basées sur les meilleures pratiques en matière de cybersécurité s'éloignent des méthodes habituelles, qui ont évoluées sur plusieurs décennies. La capacité à accepter l'évolution de son infrastructure informatique est un élément facilitateur pour mener à bien le changement, aussi bien dans la mentalité et la philosophie envers la sécurité.

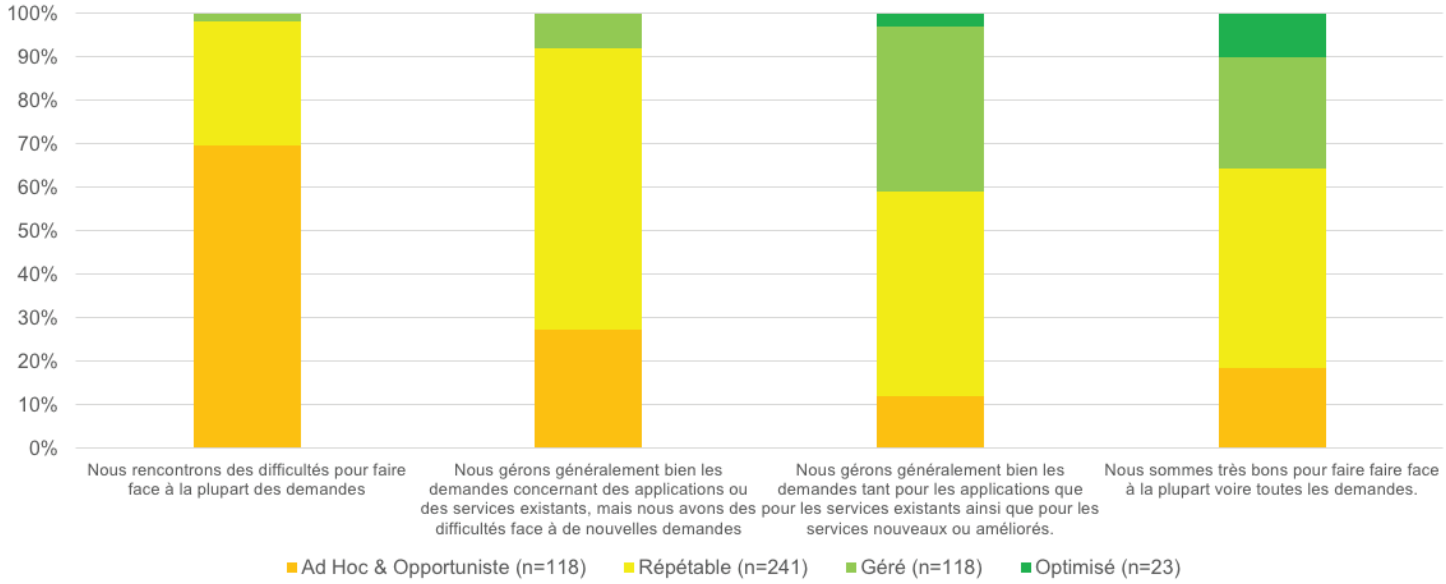
C'est ce qui est notamment mis en avant dans la transformation numérique, puisque c'est l'une des principales raisons qui pousse les entreprises dans ces eaux infestées de requins. Les pratiques standard des professionnels de la sécurité peuvent freiner l'adoption de technologies de type réseaux sociaux, mobilité Big Data/analytique et cloud computing. Certes, la mise en œuvre de ces technologies accentue l'exposition au risque. Toutefois, cette approche n'est pas mature. Plutôt que d'empêcher la transformation numérique, la démarche la plus judicieuse est de responsabiliser davantage les utilisateurs en leur fournissant les outils leur permettant d'adopter cette transformation en toute sécurité.

Comme l'illustre le graphique 4 ci-dessous, selon les critères de cette étude, plus une organisation est mature, mieux elle s'adaptera face au changement informatique. Au niveau le plus bas, les entreprises les moins matures ont des difficultés face à tout changement informatique, ou du moins, elles gèrent difficilement les demandes autres que les modifications de base des applications et des services. Toutefois, à mesure que le niveau de maturité augmente, les entreprises se décrivent comme étant plus aptes à faire face à ce changement, voire « excellentes » dans sa mise en œuvre.

Les résultats de cette étude montrent que, dans l'environnement de sécurité actuel, le dynamisme et le succès d'une entreprise reposent principalement sur une approche mature de la sécurité et la capacité à maîtriser (plutôt que craindre) le changement informatique. Il s'agit d'une démarche bilatérale, chaque composante reflétant l'autre. La capacité à conduire le changement informatique requiert une compréhension profonde des implications au niveau de la sécurité. Simultanément, pour adopter un positionnement mature vis-à-vis de la sécurité, la capacité à appliquer les changements voulus au niveau de l'environnement informatique est essentielle.

Capacité à gérer le changement par niveau de maturité en matière de cyber-risque

Q2. En ce qui concerne les demandes de l'entreprise pour des applications ou des services nouveaux ou améliorés, quelle formulation reflète le mieux les capacités de votre service informatique ?



Graphique 4 *Source: IDC, 2016*

10 RECOMMANDATIONS POUR VOTRE ORGANISATION

Les 10 recommandations suivantes offrent à votre entreprise un cadre de travail permettant d'améliorer son niveau de maturité SSI :

- **Comparez votre positionnement par rapport à vos pairs les plus proches en termes d'activité, de taille et d'implantation géographique.**
- **Déterminez quels sont vos objectifs en matière de maturité et le niveau que vous voulez atteindre.**
- **Mesurez l'écart entre votre approche actuelle de sécurité par rapport à l'état souhaité.**
- **Envisagez de faire appel à des spécialistes de la sécurité externes pour vous aider à concevoir et mettre en œuvre les changements requis pour atteindre vos objectifs.**
- **Différenciez les activités et les processus essentiels liés à la sécurité de ceux qui présentent une faible valeur et qui sont répétitifs.**
- **Identifiez les activités à faible valeur pouvant être automatisées pour réduire les ressources.**
- **Déterminez les résultats qui peuvent être améliorés en faisant appel à des MSSP. Les activités à faible valeur peuvent représenter un bon point de départ, en utilisant les modèles de prestations internationaux et industrialisés.**
- **Toutefois, l'offre de services de sécurité gérés étant désormais étendue, recherchez les expertises disponibles qui pourraient conduire aux résultats souhaités, en tenant compte du coût et de la qualité.**
- **Adoptez une approche sécurité qui prend en compte un risque à l'échelle de l'entreprise. Comme tous les utilisateurs représentent des « menaces internes » potentielles, votre culture et votre stratégie de sécurité doivent être globales.**
- **Intégrez les responsables de la sécurité dans vos nouvelles initiatives commerciales dès le début. S'assurer que les nouvelles initiatives « intrinsèquement sécurisées » simplifieront la suite des processus.**