Janvier 2023

Comment assurer la bonne gouvernance sécurité d'une entreprise ?
Emeline Diene & Victor Peraldi*

1. *Les entreprises sont-elles suffisamment protégées et que convient-il de faire pour relever le défi des cyber-menaces ?*

On estime que les entreprises ne sont pas suffisamment protégées aujourd'hui. En effet, *« il n'y a pas un rapport qui ne montre pas des statistiques catastrophiques »*. Ces statistiques viennent de deux sources, notamment les **producteurs de solutions en cyber sécurité**, qui sont fiables mais ont tendance à surestimer les chiffres des menaces ainsi que des agences (police, Interpol) qui sont fiables mais dont les chiffres sont sous-estimés en raison d'un taux de plaintes inférieur au nombre réel d'attaques.

On estime qu'en réalité, 54% des entreprises en France ont été attaquées en 2021. On constate que le *ransomware* est la menace la plus utilisée ces dernières années, avec une augmentation de leur utilisation de 255% en 2021 selon l'ANSSI, marquée par une sophistication croissante.

Il ne faut pas sous-estimer la menace, une étude de l'ONU souligne que 60% des PME attaquées ne se relèvent pas et déposent le bilan dans les 6 mois. Il y a un risque de contamination entre les différents acteurs de la *supply chain*, pouvant entrainer une perte de confiance ainsi qu'une perte d'exploitation.

2. *Comment relever le défi de la cyber menace ?*

   - C'est l'affaire de tous : Se persuader que ça n'arrive pas qu'aux autres, les petites et les grandes entreprises sont touchées
   - Investir dans des systèmes de protection car les cyber-pirates sont opportunistes et se tourneront naturellement vers des cibles moins protégées leur permettant l'utilisation d'attaques moins sophistiquées.
   - Mettre en place un système d'alerte efficace pour réagir vite, donc avoir des procédures pour être très vite en gestion de crise cyber et éviter la propagation par entre-connexion.
   - Développer des campagnes de sensibilisation régulières au sein des entreprises pour expliquer que le paysage est à risque dans un contexte où le télétravail s'est rapidement développé.

3. *Quel est le coût économique ?*

Le coût d'une crise cyber est un sujet de

- **Court terme** : perte exploitation, on ne délivre plus les services à cause de l'immobilisation des systèmes.
- **Long terme** : dégradation de l'image de l'entreprise.

- **Encore plus long** : indemnisations et amendes de certaines autorités dues à l'incapacité d'honorer ses engagements.

Il est estimé que le cout moyen d'une cyber-attaque dans le monde sur une entreprise, est de **3,5 millions de dollars**, ce qui explique la difficulté des petites entreprises à y survivre.

4. Est-ce que le mode de travail adopté au sein d'une entreprise a une influence sur les risques cyber ?

Avec le Covid on a eu recours accru au télé travail, ce qui a favorisé le développement des attaques et le fait qu'elles se répandent de manière exponentielle, notamment à cause de l'utilisation intensive des boites mail, entrainant plus de contaminations par *fishing*. Le climat de confiance ambiant au sein des entreprises et le manque de prévention favorisent la négligence des salariés.

5. *Quid du facteur humain ?*

Le facteur humain est important, il est la première barrière de défense contre les cyber-attaques. Il est nécessaire que les employés changent régulièrement leurs mots de passe et adoptent les bons réflexes.

6. *On a 15000 postes qui ne trouvent pas preneur au sein du cyber : que faire ?*

Il faut rendre ces métiers attractifs et attirer plus de jeunes dans ces métiers (mais cela prend du temps), notamment en proposant des salaires attractifs. Mais cela ne suffit pas, il faut également favoriser la reconversion professionnelle vers des compétences en cyber sécurité.

Une des solutions réside en l'**externalisation**, c'est-à-dire confier sa protection cyber à des prestataires spécialisés dans le domaine, comme Orange cyber, mais cela nécessite un niveau de confiance important dans la fiabilité du fournisseur.

L'un des avantages de cette solution consiste en la vision d'ensemble des risques qu'ont ces prestataires sur les cyber attaques susceptibles de toucher leurs clients, notamment du fait de leur large champs d'intervention. Ces prestataires sont donc de bons pourvoyeurs d'alerte (il sera plus facile de contrer une cyber-attaque ayant déjà touché un autre client).

7. *Quels sont les mécanismes de protection au niveau européen ?*

- NIS 2
- European Cyber resillience Act (CRA) : une manière de responsabiliser les fournisseurs

8. *Comment relever le défi de la cyber-protection lorsqu'on l'on est soi-même cyber-protecteur ?*

Il est nécessaire d'être exemplaire dans la protection de ses propres systèmes afin de pouvoir montrer l'efficacité de sa réaction, de sa protection et de sa fiabilité auprès du client. Il faut aussi être exigeant vis-à-vis des fournisseurs, notamment en établissant des grands principes à respecter : Une nécessité d'**information**, de **rigueur** et de **transparence** avec ses fournisseurs et clients.

9. *Est-il plus facile de sensibiliser une population ouverte au domaine du digital à ces menaces ? N'est-ce pas aussi un défi à relever sur une population ayant le sentiment de maitriser la technologie ?*

Il peut être compliqué de sensibiliser aux risques cyber quand la population est éduquée au numérique, d'autant plus que chaque entreprise a sa propre culture. Le message doit être adapté à chacune des fonctions dans l'entreprise, afin que chacun soit conscient des risques cyber propres à son activité. Il faut donc passer par la confiance, sensibiliser plutôt que d'être impératif sur les démarches à suivre. Il faut user de subtilité et travailler sur la sensibilité de l'information.

10. *Est-ce qu'Orange met en concurrence Orange Cyber avec d'autres fournisseurs ?*

Orange procède à la mise en compétition régulière de prestataires (les contrats ne sont pas tous donnés à Orange Cyber). Le groupe préfère s'assurer d'opter pour l'offre la plus adaptée aux menaces cyber.

11. *Quel rôle peuvent jouer les compagnies d'assurance ? acteur positif ?*

Assurer un risque cyber fait peser une obligation de vigilance et de maintien d'un certain niveau de protection sur les entreprises. Dans les faits, on constate cependant, que le coût moyen d'une attaque étant de 3.5 millions d'euros, les assurances préfèrent dans la majorité des cas, payer la rançon qui est toujours très inférieure à cette somme. Cette pratique a donc contribué à rendre plus attractive l'attaque par *Ransomware*, les pirates étant presque toujours assurés de la rentabilité de leur action. Les entreprises ont par ailleurs remarqué que dans un tel contexte il était plus rentable de souscrire à une assurance que d'investir dans l'amélioration de leurs défenses cyber.

12. *Quid des problématiques liées au développement des transports autonomes ?*

Il faut être plus sérieux et systématique dans la démarche Security web design. Il faut avoir une vraie chaine de confiance sur les commandes. Concernant le secteur de l'automobile il n'y a pas d'organe supra-constructeur pour gérer la sécurité de tous les véhicules, chaque groupe a son mode de surveillance ce qui complexifie la supervision et l'établissement de règles communes à ce secteur.

Dans l'aviation cela devrait se synchroniser plus facilement car cette industrie repose essentiellement sur deux grands constructeurs, ce qui facilite une stratégie sécuritaire commune.

*Emeline Diene, Victor Peraldi - CEPS