



Cybersécurité : protégeons nos données !

MAI 2018



Sommaire

Préambule	2
I. La donnée, un actif à défendre	4
Nouvelles opportunités, nouvelles menaces	5
Des impacts aux conséquences mal maîtrisées	8
Le temps long de la réglementation	10
II. Un éclairage d'expert sur la cybersécurité : entretien avec Worldline	12
III. La cybersécurité, un axe fort de notre démarche de dialogue avec les entreprises	16
Une approche structurée de la stratégie digitale des entreprises	17
La cybersécurité, source de dialogue avec les entreprises	19
Glossaire	20
Références	21
A propos de ODDO BHF Asset Management	21

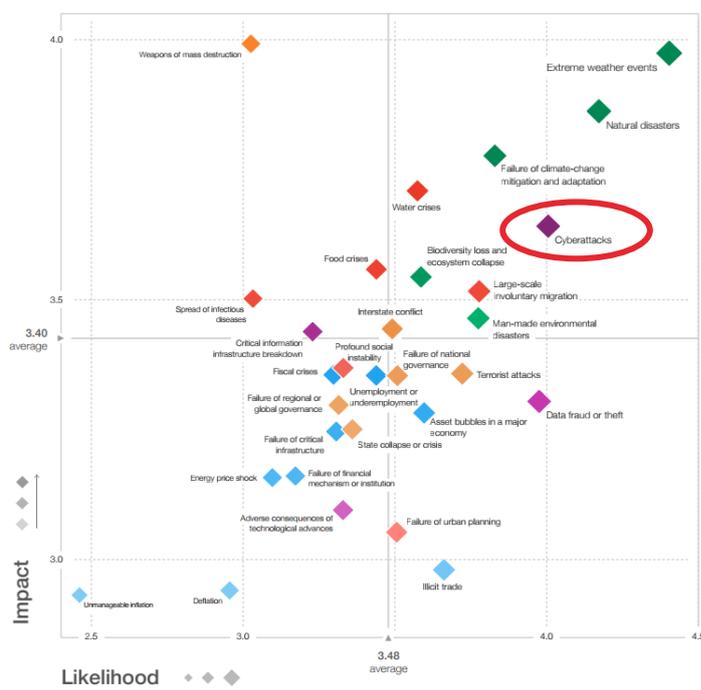
Préambule

La numérisation de l'économie bouleverse depuis une vingtaine d'années les habitudes de travail, de consommation ainsi que les relations entre individus et/ou organisations. Les entreprises ont dû s'adapter aux exigences de rapidité, de mobilité, de connectivité ou même encore de virtualisation imposées par ce nouvel environnement. L'économie numérique contribue désormais pour plus de 30% à la croissance du PIB des pays développés et **la donnée est devenue un actif stratégique à valoriser mais aussi à défendre.**

« *Le coût de la cybercriminalité pour l'économie mondiale pourrait atteindre 8 000 Md\$ d'ici 2022* »

Avec environ 3.9 milliards d'utilisateurs d'internet dans le monde et 8.4 milliards d'objets connectés, la cybersécurité est devenue en quelques années un enjeu majeur pour les dirigeants d'entreprises, comme en témoigne la dernière enquête¹ du Forum Economique Mondial sur la cartographie des risques pour 2018.

Cartographie des risques pour 2018



Source : Forum Economique Mondial

1 http://www3.weforum.org/docs/WEF_GRR18_Report.pdf



Le coût de la cybercriminalité pour l'économie mondiale pourrait atteindre 8 000 Md\$ d'ici 2022 selon l'étude, soit près de la moitié du PIB de l'Union Européenne. L'année 2017 a d'ailleurs été marquée par deux attaques d'ampleur : WannaCry (300 000 ordinateurs infectés dans 150 pays) et NotPetya (qui a touché plusieurs entreprises en Ukraine, Russie, Europe et Etats-Unis). D'après une étude du cabinet Deloitte publiée en janvier 2018, **75% des entreprises interrogées affirment avoir adopté de nouvelles mesures de sécurité après ces deux attaques**. La cybercriminalité engendre donc des coûts internes de plus en plus importants pour les entreprises (investissements IT et humains essentiellement) mais aussi des coûts externes difficilement mesurables (vol de données, pertes de revenus, interruption d'activité, risque de réputation).

Les cibles des cybercriminels sont multiples, de la propriété intellectuelle aux données financières, mais la majorité des attaques se concentrent sur les données personnelles. La hausse exponentielle des objets connectés en circulation offre en effet un champ d'action exceptionnel.

Si les premières réglementations visant à protéger l'utilisation des données personnelles remontent à près de 50 ans (en 1970 dans le Land de Hesse en Allemagne, en 1973 en Suède, en 1978 en France), ce sont aujourd'hui plus de 100 pays qui se sont dotés d'une législation sur le sujet. A ce titre, l'année 2018 marque une évolution importante en Europe, **avec l'entrée en vigueur le 25 mai du Règlement Général sur la Protection des Données (RGPD)**, venant remplacer la Directive sur la Protection des Données (DPD) de 1995.

« Montée en puissance des cyber-risques et impact pour les entreprises font de la cybersécurité un axe fort de notre démarche de dialogue »

La digitalisation de l'économie apporte indéniablement de nouvelles opportunités de développement dans de nombreux secteurs d'activité, mais aussi de nouveaux risques dont les contours et les conséquences sont incertains et en perpétuelle évolution.

La montée des cyber-risques, devenue inexorable par la transformation numérique de l'économie, rend l'analyse de cette composante indispensable dans le travail d'analyse financière et extra-financière d'une entreprise. ODDO BHF Asset Management l'intègre d'ores et déjà dans son modèle d'analyse ESG et la cybersécurité fait désormais partie des sujets récurrents que nous abordons dans notre démarche de dialogue avec les entreprises.



Nicolas Jacob

Head of ESG Research, ODDO BHF Asset Management SAS



La donnée, un actif à défendre



« La donnée est le nouveau pétrole. Elle a de la valeur mais ne sert pas à grand-chose si elle n'est pas raffinée. Le pétrole doit être transformé si on veut l'utiliser efficacement. Il en va de même pour la donnée qui doit être déconstruite puis analysée pour offrir de la valeur »

Clive Humby, mathématicien britannique et pionnier du Big Data, 2006

En 2017, une minute sur internet a représenté 18 millions de personnes cherchant la météo, 3.6 millions de recherches Google, 4.1 millions de vidéos regardées sur YouTube, 527 760 photos partagées sur Snapchat ou bien encore 103 millions de spams envoyés à travers le monde².

Nouvelles opportunités, nouvelles menaces

La quantité de données collectées croît à un rythme annuel moyen supérieur à 50% depuis 10 ans, ouvrant un champ d'analyse colossal pour les entreprises sur l'ensemble de la chaîne de valeur. Cet univers de données, appelé « Big Data », se caractérise par le fait que de plus en plus de données disponibles et collectées sont « non-structurées », c'est-à-dire issues de supports mobiles, de plateformes d'échange sur internet, des réseaux sociaux ou bien encore des objets connectés. Aujourd'hui, plus de 90% des données issues de l'univers digital sont non-structurées, illustrant bien l'effet multiplicateur du Big Data.

« Un triple enjeu à gérer pour l'entreprise : la collecte, le stockage et le traitement de la donnée »

Savoir traiter cette masse de données peut être une source de valeur ajoutée pour les entreprises comme le montre une note publiée en novembre 2013³ par le cabinet McKinsey, estimant qu'une bonne stratégie digitale pouvait avoir des impacts positifs significatifs sur les résultats à un horizon de 5 ans, de 20% en moyenne via une plus forte croissance de revenus et de 36% en moyenne via l'optimisation des coûts (gains de productivité).

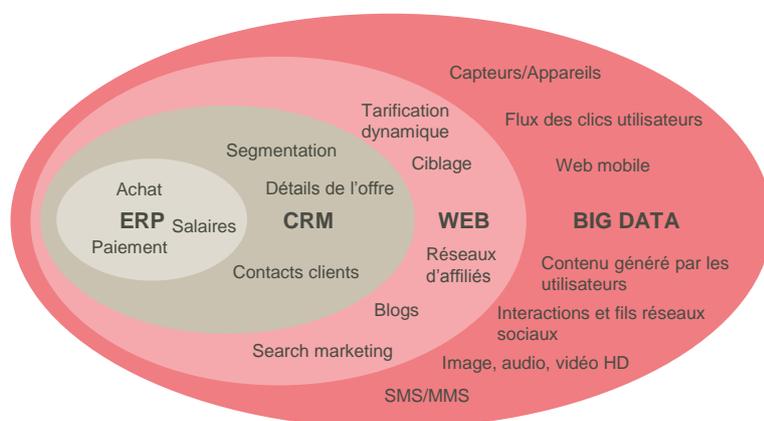
Dans le processus de transformation digitale, la donnée est donc devenue un actif essentiel pour l'entreprise. Mais avant d'en tirer avantage, elle doit faire face à un triple challenge : la collecte, le stockage et le traitement de la donnée.

Les organisations qui sauront en tirer profit pourront bénéficier d'un avantage compétitif.

² Source : Byothe.fr

³ "Finding your digital sweet spot", McKinsey, Novembre 2013

L'univers en croissance de la donnée



Sources : Teradata, ODDO BHF Asset Management

A contrario, la puissance économique de la donnée en fait un actif de plus en plus convoité et par conséquent source d'attaques malveillantes voire criminelles. **Sur la seule année 2017, environ 700 millions de cyber-attaques ont eu lieu**, soit un doublement depuis 2015. D'après le rapport 2018 sur la sécurité des données publié par Thales et le cabinet 451 Research⁴, 67% des 1200 responsables de la sécurité informatique interrogés au niveau mondial affirment avoir déjà subi un vol de données dans le passé.

« Le développement des objets connectés et l'intelligence artificielle vont provoquer davantage de cyber-attaques venant de l'extérieur »

Les cyber-menaces peuvent être de nature très différentes, rendant leur anticipation et leur gestion très complexes pour toute organisation. Le premier niveau d'analyse est d'abord de distinguer autant les menaces internes à l'entreprise, encore souvent sous-estimées, que les menaces externes. Si l'importance de l'une ou de l'autre est très variable en fonction des méthodes employées et de leurs conséquences, leur nombre ne fait que s'amplifier avec le développement technologique. A titre d'illustration, la croissance en volume des objets connectés et le développement de l'intelligence artificielle vont générer un nombre croissant d'attaques externes. De la même façon, le développement de la pratique du « bring your own device » (qui consiste à autoriser les employés à utiliser leurs appareils personnels pour accéder aux données de l'entreprise) devient un défi majeur pour la sécurité des systèmes informatiques d'une entreprise.

4 « 2018 Thales data threat report », Thales et 451 Research, Janvier 2018



Des cyber-menaces protéiformes



Source : ODDO BHF Asset Management

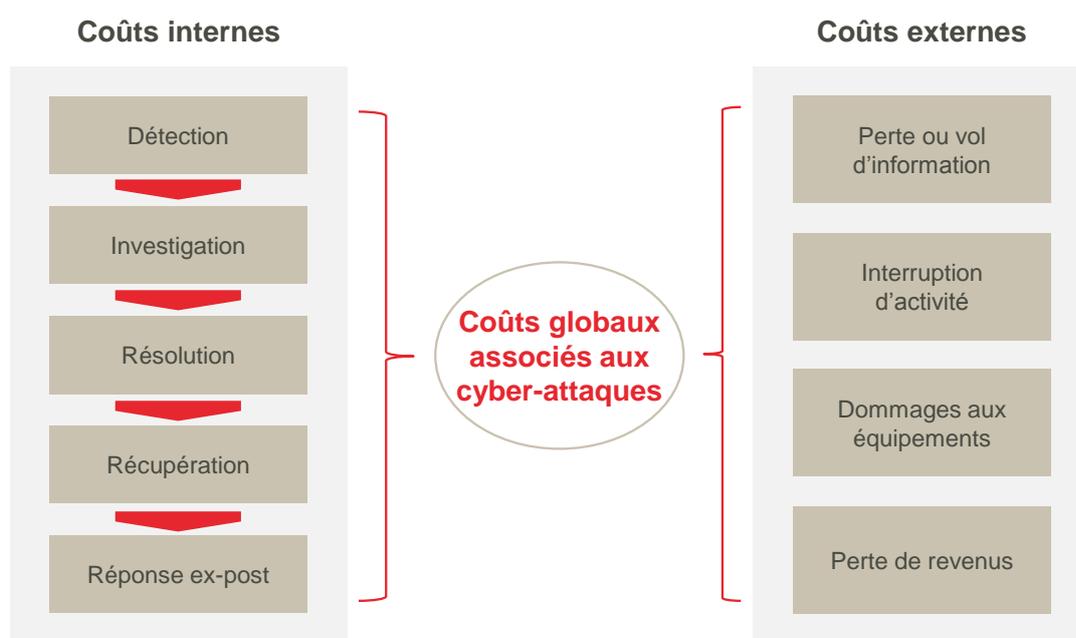
Le développement des technologies mobiles et des objets connectés ont généré ces dernières années un grand nombre de **données personnelles qui sont devenues les cibles privilégiées des cyber-attaquants**. Sans surprise, les domaines les plus attaqués sont les secteurs tournés vers le client final (utilisateur ou consommateur), tels que l'information et la communication (96% des attaques externes concernent les données personnelles), le commerce de détail (91%) et les services financiers (42%)⁵.

5 Source : IBM X-Force Threat Intelligence Index 2017

Des impacts aux conséquences mal maîtrisées

Les désormais célèbres cyber-attaques intervenues en 2017 (Wannacry et NotPetya) ont montré que les impacts ne se limitaient plus à la gestion du vol ou de la perte de données. **Elles s'étendent désormais progressivement aux atteintes à la réputation d'une entreprise, aux coûts associés à une perte d'exploitation ou bien encore à une perturbation d'infrastructures critiques.** NotPetya, ransomware⁶ déclenché en juin 2017, a d'abord sérieusement impacté le fonctionnement des administrations et infrastructures ukrainiennes avant de toucher de nombreuses entreprises privées présentes dans le pays mais aussi les sociétés hors d'Ukraine ayant des filiales locales. Parmi celles ayant publiquement communiqué, le danois A.P. Moeller Maersk et le britannique Reckitt Benckiser ont respectivement perdu 250 et 100 millions de dollars, soit de 4 à 10% de leur résultat d'exploitation.

Coûts potentiels d'une cyber-attaque pour les entreprises



Sources : Accenture, Ponemon

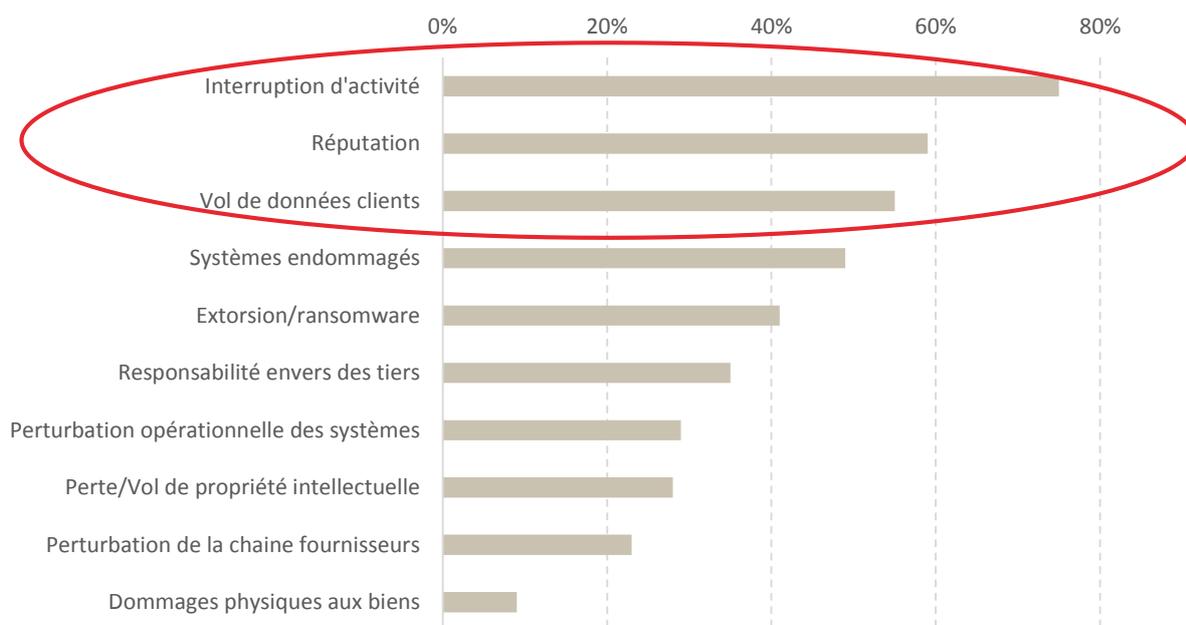
Cette tendance se reflète dans l'évolution des préoccupations des entreprises. En février 2018, le cabinet Marsh en association avec le groupe Microsoft publiait les résultats d'une étude menée auprès de 1300 décideurs d'entreprises sur les cinq continents sur la perception des cyber-risques, montrant un net déplacement des préoccupations des sujets internes (gestion IT par exemple) vers les conséquences potentielles sur l'ensemble de la chaîne de valeur de l'entreprise (interruption d'activité, réputation, vol de données clients).

6 Voir glossaire



« Des impacts potentiels sur l'ensemble de la chaîne de valeur »

Scénarios les plus redoutés par les entreprises sur les conséquences d'une cyber-attaque



Source : Marsh and Microsoft Cyber perception survey, 2018

L'affaire Facebook/Cambridge Analytica, rendue publique en mars 2018⁷, interroge même sur les fondements et la pérennité d'un modèle d'affaire reposant exclusivement sur la collecte, le stockage et la valorisation des données personnelles. L'affaire a mis au jour le fait qu'une utilisation des données des utilisateurs à leur insu peut entraîner une perte de confiance et générer des impacts négatifs durables sur la réputation de l'entreprise.

« Nous avons une responsabilité : protéger vos données. Si nous n'y parvenons pas, nous ne méritons pas votre confiance »

Mark Zuckerberg, dirigeant-fondateur de Facebook, mars 2018

Il reste pour le moment que le coût global d'une cyber-attaque est difficile à évaluer d'autant plus que **la part des actifs intangibles dans la valorisation des entreprises est croissante**, cela rendant encore plus complexe toute tentative d'estimation à court terme.

⁷ Cambridge Analytica, société américaine de communication stratégique, a siphonné via le réseau social Facebook les données personnelles de plus de 80 millions de personnes entre 2014 et 2016

Le temps long de la réglementation

Si les ruptures technologiques apportent toujours de puissants relais de croissance, elles créent aussi bien souvent de nouveaux risques ignorés dans un premier temps par la réglementation. La digitalisation n'échappe à la règle et le processus d'adaptation législative obéit à un temps bien plus long que le développement des pratiques frauduleuses voire criminelles.

Les cyber-risques ont connu une croissance exponentielle au début des années 2010, accompagnant l'accélération de la numérisation de l'économie. **C'est dans ce contexte que le Parlement Européen a voté en avril 2016 un projet de règlement visant à revoir et à renforcer les mécanismes de protection des données** (régis par les droits nationaux en adaptation de la Directive de 1995). Ce règlement sur la protection des données (RGPD) est applicable immédiatement, à la différence d'une directive qui doit être transposée en droit national, à compter de son entrée en vigueur en mai 2018.



Le Règlement Général sur la Protection des Données (RGPD)

Le RGPD est le texte de référence en matière de **protection des données personnelles** au niveau de l'Union européenne. Cet ensemble de règles remplace un précédent texte datant de 1995 (Directive 95/49/CE), devenu inadapté dans un environnement numérique en forte croissance.

Toutes les organisations (publiques ou privées) basées dans l'Union européenne ou situées hors-UE mais gérant les données personnelles de résidents européens devront être en **conformité avec le RGPD** d'ici au 25 mai 2018.



Les dispositions clés à retenir :

- La notion de **consentement explicite** : les organisations publiques et les entreprises privées doivent s'assurer du consentement explicite des utilisateurs avant de recueillir leurs données personnelles ;
- La notion de **droit à l'effacement** (ou « droit à l'oubli ») : chaque citoyen de l'UE a le droit de demander l'effacement de tout ou partie de ses données personnelles par le responsable du traitement de ces données, en raison de plusieurs motifs (par exemple en cas de traitement illicite ou de retrait du consentement) ;
- La notion de **portabilité des données** : toute personne est en droit de récupérer ses données personnelles auprès de l'organisme qui les a recueillies, dans un format structuré et couramment utilisé afin de transmettre ces données à tout autre responsable de traitement de son choix ;
- La notion de **notification des fuites** : en cas de piratage informatique, le responsable du traitement doit en notifier l'autorité nationale de protection des données ainsi que les utilisateurs affectés ;
- L'obligation faite aux organismes publics (et aux entreprises privées de plus de 250 salariés) de nommer un **délégué à la protection des données** (ou Data Protection Officer) ;
- La notion de protection des données **dès la conception** : les exigences relatives à la protection des données doivent être prises en compte, par les organismes publics ou entreprises privées, dès le stade de la conception de leurs produits, services et systèmes. Le but de cette disposition est de **protéger les données des utilisateurs** de façon à ce qu'elles ne puissent pas être divulguées à de tierces personnes, ni à permettre à celles-ci de tout connaître de la vie privée des utilisateurs.

Le chantier de mise en conformité avec le RGPD est un sujet complexe dont la mise en œuvre pourrait exiger des délais et des changements importants dans les entreprises. Cependant, à partir du 25 mai 2018, les entreprises ont à charge de prouver qu'elles respectent les dispositions prévues par le RGPD et notamment les changements afférents à la traçabilité et à la cartographie des traitements des données personnelles qui découlent des nouvelles règles de la protection des données.

Faute d'avoir respecté cette mise en conformité, les entreprises s'exposent à une sanction financière pouvant aller jusqu'à 20 M€ ou 4 % de leur chiffre d'affaires annuel mondial.





Un éclairage d'expert sur la cybersécurité : entretien avec Worldline



La digitalisation de l'économie a fait basculer le monde dans l'ère de la donnée à grande échelle. Concomitamment à ce mouvement, la cybercriminalité s'est développée et perfectionnée, touchant un nombre toujours plus important d'organisations et d'individus. Des événements récents tels que l'affaire Facebook/Cambridge Analytica nous montre que la cybersécurité devient le socle de la confiance.

Nous remercions vivement les experts de la société Worldline, leader dans le secteur des paiements électroniques et des services transactionnels, de nous avoir apporté des réponses précises et essentielles à la bonne compréhension de la thématique cyber-sécurité.

ODDO BHF AM : En tant qu'acteur de premier plan dans les technologies des paiements électroniques, quel regard portez-vous sur les cyber-risques sur un horizon de 5 à 10 ans ?

Worldline : La cybersécurité est au cœur de notre modèle d'affaire et est devenue depuis quelques années le sujet le plus sensible dans notre cartographie des risques, aussi bien en termes d'impact potentiel sur nos activités que sur la probabilité de survenance. Le sujet est d'ailleurs discuté chaque mois au sein du Comité de direction autour de KPI spécifiques. Le domaine des paiements électroniques est très sensible par nature mais soumis à une norme stricte, le PCI DSS (Payment Card Industry Data Security Standard), créé en 2004 par les principaux fournisseurs de cartes de paiement afin d'augmenter le contrôle des informations des titulaires de cartes et réduire les utilisations frauduleuses des instruments de paiement. Concrètement, il s'agit essentiellement de fractionner et de crypter les données afin qu'aucun intervenant de la chaîne de paiement ne conserve trop de données. Dans ce domaine, le vol de données est donc toujours possible mais compliqué à organiser. Parmi les menaces plus difficiles à cerner car beaucoup plus simple à

mettre en œuvre, les attaques dites DDoS (Distributed Denial of Service) ou attaques par « déni de service distribué » consistent à rendre impossible l'accès à un serveur web par saturation. En coupant le service, l'attaquant cherche à porter un préjudice financier à une entreprise ou à une marque et à nuire à sa réputation. Le spectre des cyber-menaces est donc large, mais les plus préoccupantes sont probablement celles qui visent à la déstabilisation des organisations, entreprises ou entités publiques.

ODDO BHF AM : Combattre les nouvelles menaces technologiques par la technologie semble être la solution. Comment voyez-vous se développer la cryptologie ?

Worldline : Dans les paiements électroniques, toutes les données échangées sont cryptées. Ce processus fait partie intégrante de la conformité de ce type de service via l'application de la norme PCI DSS, même si celle-ci n'est applicable qu'à partir de certains seuils de chiffre d'affaires. Pour autant, les technologies de chiffrement évoluant régulièrement, des difficultés se posent quant à la façon de travailler avec les clients, certains

secteurs ayant des difficultés d'adaptation. Le coût de mise à jour permanente des technologies pour intégrer les versions les plus à jour des technologies de chiffrement peut devenir un obstacle économique important pour des acteurs de taille modeste du e-commerce notamment, et par la suite générer des difficultés opérationnelles d'intégration avec leurs grands partenaires. La technologie est donc efficace et maintenant largement éprouvée, mais son déploiement à très grande échelle reste ralenti par des réalités et des contraintes économiques très différentes d'un secteur d'activité à un autre.

ODDO BHF AM : Le développement de la blockchain peut-il également apporter des réponses en matière de cybersécurité ?

Worldline : Par l'absence d'intermédiaire, la technologie blockchain est sûre par nature. S'agissant d'une chaîne de blocs d'informations fractionnées et vérifiées par les utilisateurs eux-mêmes, toute attaque extérieure est rendue très difficile, au moins pour les blockchains privées. Néanmoins, cette technologie est encore loin de la maturité et présente toujours des freins à son développement tels que l'absence de temps réel, le coût de mise en œuvre, ou bien encore un niveau de consommation énergétique très élevé (plus la chaîne est grande, plus les ressources IT sont importantes et plus la consommation énergétique est élevée). La marche est encore haute pour une application large type e-commerce compte tenu de la taille des bases de données à gérer et de leur caractère évolutif. En revanche, cette technologie fait ses preuves en environnement fermé. C'est dans cette logique par exemple que Bureau Veritas a lancé en mars

2018 en partenariat avec Worldline le premier label de traçabilité alimentaire reposant sur la blockchain permettant ainsi aux consommateurs d'avoir accès aux informations de chaque étape de fabrication d'un produit. Dans ce cas, la nature des données est clairement définie et répétitive.

ODDO BHF AM : L'entrée en vigueur du Règlement Général sur la Protection des Données (RGPD) au sein de l'Union Européenne semble soit sous-estimé par nombre d'entreprises, en particulier les plus petites, soit méconnu par la majorité des citoyens. Dans un contexte de défiance du consommateur quant au traitement de ses données personnelles, quelle est selon vous la principale rupture par rapport à la législation actuelle ?

Worldline : Le RGPD impacte la chaîne de valeur dans son ensemble. Beaucoup d'échanges d'informations ne sont pas contractualisés aujourd'hui. Le renforcement de la responsabilité de chaque partie prenante dans la collecte et le traitement de la donnée va entraîner des modifications importantes dans les façons de travailler, de structurer l'information et dans l'exercice des contrôles. Pour les modèles d'affaire BtoC s'ajoutera le devoir de s'assurer du consentement explicite du consommateur et d'être en mesure de répondre à de nouveaux droits tels que le droit à l'oubli, à la portabilité ou d'opposition à certaines activités de traitement des données personnelles. Toute entreprise sera également responsable du traitement des données personnelles de ses collaborateurs impliquant probablement une remise à plat de nombreux processus RH.



ODDO BHF AM : Pensez-vous que le RGPD contribuera à renforcer la cybersécurité via notamment une meilleure traçabilité et une responsabilité qui incombera désormais clairement aux détenteurs des données ?

Worldline : Oui, sans aucun doute. Il faut bien garder à l'esprit que les deux tiers des obligations découlant de la mise en œuvre du RGPD relèvent du contrôle et de la gestion des risques, le tiers restant concernant des éléments opérationnels directement liés aux systèmes d'informations. Le passage d'une logique de conformité à une logique de responsabilité et les potentielles sanctions financièrement dissuasives en font véritablement un sujet transversal pour toute organisation nécessitant une implication à tous les niveaux hiérarchiques. Un des fondements de ce nouveau règlement est de redonner confiance dans la collecte et le traitement de la donnée et les moyens à mettre en œuvre vont clairement dans le sens d'une meilleure maîtrise des cyber-risques.



La cybersécurité, un axe fort
de notre démarche de
dialogue avec les entreprises



Notre modèle interne d'analyse ESG des entreprises accorde historiquement une place importante à l'étude des actifs intangibles et du capital immatériel tels que le capital humain, l'innovation ou bien encore le capital organisationnel (client, marque, fournisseurs, technologie). Au sein de ce dernier, **nous intégrons une approche systématique de la stratégie digitale des entreprises, source d'opportunités mais aussi de risques opérationnels à moyen terme.**

La montée en puissance des cyber-risques comme sujet de préoccupation des dirigeants d'entreprise et leur impact de plus en plus matériel pour l'investisseur **font désormais de la cybersécurité un axe fort de notre démarche de dialogue avec les entreprises.**

Une approche structurée de la stratégie digitale des entreprises

L'usage des nouvelles technologies change radicalement le fonctionnement traditionnel de l'entreprise, quel que soit le secteur d'activité, de par la multiplication des interactions et le raccourcissement exceptionnel des délais de traitement de l'information. La stratégie digitale de l'entreprise peut et doit trouver des applications concrètes aussi bien en amont (gestion des coûts, processing, RH, fournisseurs) qu'en aval (marketing, distribution) de l'activité.

Pour certaines entreprises, la stratégie avale est centrale et la majorité des efforts doit porter sur le client. A contrario, pour bon nombre d'entreprises industrielles, la priorité digitale doit porter sur l'amont et l'amélioration des process tant au niveau de la production, de la chaîne d'approvisionnement, que de la gestion des ressources humaines.

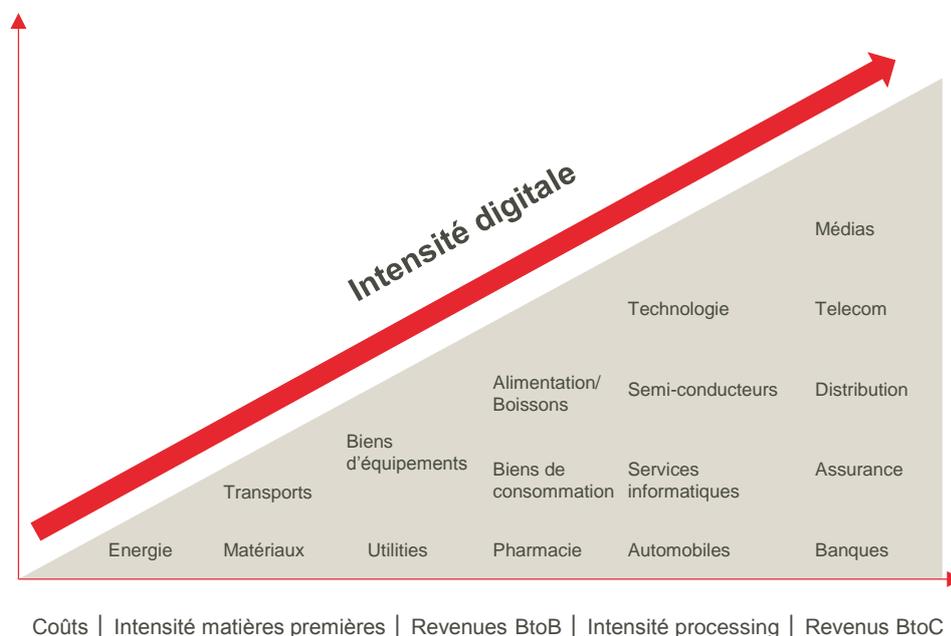
Le déploiement d'une stratégie digitale dépend donc du positionnement de chaque entreprise dans la chaîne de valeur.

« Première étape : définir l'intensité digitale de chaque secteur »

Dans notre modèle d'analyse ESG, la première étape est donc d'affecter une pondération différente à chaque secteur selon son degré d'exposition aux enjeux numériques autour de trois variables :

- Exposition coûts vs revenus,
- Exposition BtoB vs BtoC,
- Intensité matières premières vs processing (RH, fonctions back office ...).

Intensité digitale des secteurs



Source : ODDO BHF Asset Management

« Deuxième étape : analyser la stratégie digitale de chaque entreprise »

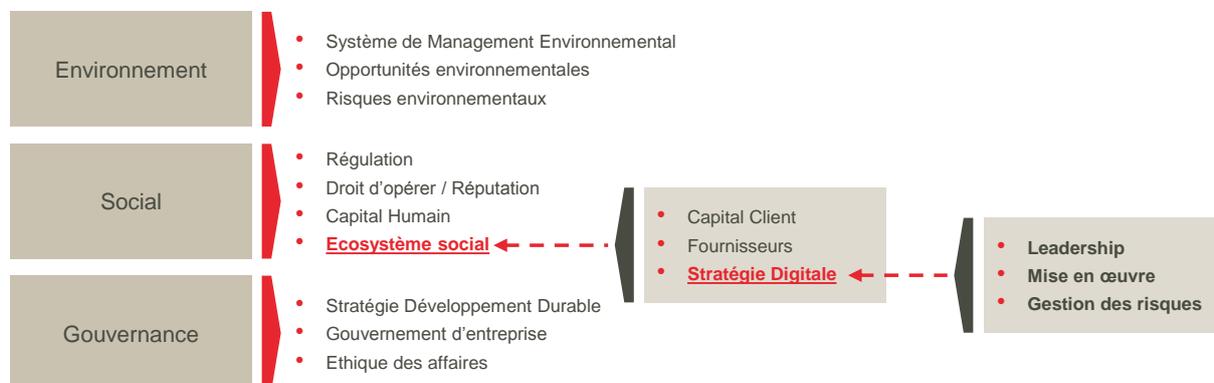
Dans un second temps, nous analysons trois critères au niveau de chaque entreprise :

- **Le leadership** : il s'agit d'identifier qui porte au sein de l'entreprise la responsabilité de la stratégie digitale et par conséquent la question de la cybersécurité (CEO, Comité exécutif, expertise présente au Conseil).
- **Le déploiement et les moyens mis en oeuvre** : nous suivons un certain nombre d'indicateurs tels que :
 - l'évolution des dépenses IT,
 - la présence d'une équipe/fonction digitale,
 - la mise en place de formations dédiées pour les employés,
 - ou bien encore l'obtention de certifications type ISO 27001 (sécurité des systèmes d'information) ou ISO 20000 (production et exploitation informatique).
- **La gestion des risques** : nous menons une analyse plus qualitative sur les moyens de défense mis en oeuvre (déploiement de technologies type cryptage des données ou processus d'authentification forte⁸, cyber-assurance) et sur l'historique des incidents éventuels en matière de protection des données.

⁸ Voir glossaire



Intégration de la stratégie digitale dans notre modèle d'analyse ESG



Source : ODDO BHF Asset Management

La cybersécurité, source de dialogue avec les entreprises

Dans sa politique d'intégration ESG, ODDO BHF Asset Management privilégie de façon générale une démarche de dialogue avec les entreprises plutôt que d'exclusion. La digitalisation de l'économie apporte indéniablement de nouvelles opportunités de développement dans de nombreux secteurs d'activité, mais aussi de nouveaux risques dont les contours et les conséquences sont incertains et en perpétuelle évolution.

Nous incitons nos équipes de gestion à traiter ce sujet dans leur exercice régulier de rencontre avec les émetteurs. **Le thème de la cybersécurité est désormais abordé systématiquement et selon la pertinence de l'enjeu par secteur auprès des entreprises avec lesquelles nous engageons un processus de dialogue sur les questions ESG.**

Glossaire

Botnet : contraction en anglais de « robot » et « réseau », un botnet est un réseau composé d'un grand nombre d'ordinateurs dont un logiciel malveillant a pris possession pour servir les intérêts du pirate informatique qui l'a créé. En prenant le contrôle de centaines ou de milliers d'ordinateurs, les botnets sont habituellement utilisés pour envoyer des virus, voler des données personnelles ou réaliser des attaques en déni de services distribués. Ils sont actuellement considérés comme l'une des plus grandes menaces en ligne.

Cryptage : procédé de chiffrement afin de rendre la compréhension d'un document impossible à toute personne et/ou système qui n'a pas la clé de déchiffrement. Ce principe est généralement lié au principe d'accès conditionnel.

Données personnelles : se définit comme toute information identifiant directement ou indirectement une personne physique (nom, numéro d'immatriculation, numéro de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale...).

Hacking : recherche et exploitation des failles dans un système ou réseau informatique, souvent afin d'obtenir un gain financier.

Ingénierie sociale : manipulation psychologique destinée à inciter des individus à divulguer des informations confidentielles.

Malware : abréviation de « malicious software », programme créé pour infecter et endommager un ordinateur.

Phishing : tentative d'obtenir des informations sensibles en se faisant passer pour une entité digne de confiance dans une communication électronique.

Processus d'identification forte : procédure d'identification qui requiert la succession d'au moins deux facteurs (ou chaînes de caractères) d'authentification.

Ransomware : logiciel malveillant conçu pour bloquer l'accès à un système informatique ou à des données jusqu'à paiement d'une somme d'argent, souvent en crypto monnaie.



Références

« Guide sur le Règlement Européen relative à la protection des données personnelles », Bird&Bird, Avril 2017

« Enjeux Cyber 2018 : L'évolution de la menace Cyber », Deloitte, Janvier 2018

« Faire face aux menaces cyber », Lloyd's of London, Septembre 2016

« 2018 Thales data threat report », Thales et 451 Research, Janvier 2018

« 2017 cost of cybercrime study », Accenture et Pnemom Institute, 2017

« The Global Risks Report 2018 », World Economic Forum, Janvier 2018

« Règlement (UE) 2016/679 du Parlement Européen et du Conseil », Journal officiel de l'Union européenne, Mai 2016

A propos de ODDO BHF Asset Management

ODDO BHF Asset Management fait partie du groupe financier franco-allemand ODDO BHF fondé en 1849.

ODDO BHF AM est un leader indépendant de la gestion d'actifs en Europe. Il regroupe les entités ODDO BHF AM SAS (France), ODDO BHF Private Equity (France) et ODDO BHF AM GmbH (Allemagne) qui, ensemble, gèrent des actifs totalisant près de 61 milliards d'euros.

ODDO BHF AM propose à ses clients institutionnels et distributeurs une gamme unique de solutions d'investissement performantes couvrant les principales classes d'actifs, les actions européennes, les stratégies quantitatives, les obligations, les solutions d'allocation d'actifs et les actifs non-cotés.

Sur une base agrégée, 70% des actifs sous gestion proviennent de clients institutionnels et 30% de partenaires de distribution. Les équipes opèrent à partir des centres d'investissement de Düsseldorf, Francfort et Paris avec des implantations supplémentaires au Luxembourg, à Milan, Genève, Stockholm et Madrid.

ODDO BHF AM met l'accompagnement de ses clients sur le long terme au cœur de ses priorités. Son indépendance permet aux équipes d'être réactives, flexibles et innovantes afin de trouver en permanence des solutions adaptées aux besoins des clients.

Disclaimer

ODDO BHF AM est la branche de gestion d'actifs du Groupe ODDO BHF. Elle est la marque commune des trois sociétés de gestion juridiquement distinctes ODDO BHF AM SAS (France), ODDO BHF Private Equity (France) et ODDO BHF AM GmbH (Allemagne).

Ce document, à caractère promotionnel, est établi par ODDO BHF ASSET MANAGEMENT SAS. **Sa remise à tout investisseur relève de la responsabilité de chaque commercialisateur, distributeur ou conseil.**

L'investisseur potentiel est invité à consulter un conseiller en investissement avant d'investir dans une stratégie. L'attention de l'investisseur est attirée sur le fait que toutes les stratégies présentées ne sont pas autorisées à la commercialisation dans tous les pays. L'investisseur est informé que les stratégies présentent un risque de perte en capital, mais aussi un certain nombre de risques liés aux instruments/stratégies en portefeuilles. En cas d'investissement, l'investisseur doit obligatoirement prendre connaissance de manière détaillée des risques encourus dans chaque stratégie. La valeur de l'investissement peut évoluer tant à la hausse qu'à la baisse et peut ne pas lui être intégralement restituée. L'investissement doit s'effectuer en fonction de ses objectifs d'investissement, son horizon d'investissement et sa capacité à faire face au risque lié à la transaction. ODDO BHF ASSET MANAGEMENT SAS ne saurait également être tenue pour responsable de tout dommage direct ou indirect résultant de l'usage de la présente publication ou des informations qu'elle contient. Les informations sont données à titre indicatif et sont susceptibles de modifications à tout moment sans avis préalable.

A compter du 3 janvier 2018, lorsque OBAM fournit des services de conseil en investissement, veuillez noter que celui-ci est toujours fourni sur une base non indépendante conformément à la directive européenne 2014/65 / UE (dite «directive MIFID II»). Veuillez également noter que toutes les recommandations faites par OBAM sont toujours fournies à des fins de diversification.



ODDO BHF Asset Management SAS

12 boulevard de la Madeleine

75440 Paris Cedex 09 France

am.oddo-bhf.com