INSTITUT DE FINANCEMENT DU DÉVELOPPEMENT DU MAGHREB ARABE

معهد تمويل التنمية للمغرب العربي

Mémoire de fin d'Etudes

Thème :

ASSURANCE DES RISQUES CYBERNÉTIQUES EN ALGÉRIE

Présenté et soutenu par :

Yousra ALIKECHE

Encadré par :

Mr. Rassem KTATA

Etudiant(e) parrainé(e) par :

La Compagnie Algérienne des Assurances CAAT

Remerciement

La réalisation de ce mémoire a été possible grâce au concours de plusieurs personnes à qui je voudrais témoigner toute ma reconnaissance.

Je voudrais tout d'abord adresser ma gratitude à mon encadrant, ***Mr Rassem KTATA,*** Chief Actuary and Chief Risk Officer de GAT assurance, pour avoir accepté de diriger ce travail, ses très nombreux commentaires, ses judicieux conseils et sa grande patience m'ont considérablement aidé dans l'élaboration de ce mémoire.

Je remercie également mon tuteur de stage ***Mr Hocine BOUAROUR***, le directeur général adjoint chargé des affaires techniques et commerciales de la ***CAAT,*** pour le privilège qu'il m'a fait en acceptant de diriger ce travail, son soutien, sa clairvoyance et ses compétences m'ont été d'une aide inestimable.

Je tiens à remercier en particulier ***Mr Younes TABOURI,*** le sous-directeur production transport à la ***CAAT,*** pour sa gentillesse, sa modestie et l'accueil cordial qu'il m'a toujours réservé m'ont inspiré une grande admiration à son égard.

Je désire aussi remercier les professeurs que j'ai eu la chance de rencontrer tout au long de mon cursus, pour leur enseignement, leurs conseils ainsi que leur disponibilité, et toute l'équipe de la direction générale de ***L'IFID***, qui m'ont fourni les outils nécessaires à la réussite de cette formation.

Enfin, mes plus grands remerciements vont à la compagnie qui a cru en mes capacités et qui m'a parrainé, ***MERCI LA CAAT***

SOMMAIRE

LISTE DES FIGURES

LISTE DES TABLEAUX

INTRODUCTION GÉNÉRALE

INTRODUCTION GÉNÉRALE

La fin du 19ème siècle a vu naitre l'informatique, « *la science qui traite de manière rationnelle toutes sortes d'informations, par l'utilisation de machine automatisée* », et le 20ème se développer de manière exponentielle. À tel point, que presque chaque aspect de notre vie peut à présent faire l'objet d'une information numérique. De fait, la consommation et l'utilisation quotidienne et massive d'outils numériques, comme les applications pour Smartphones, l'échange de données bancaires, l'envoie de courriels entraînent une explosion du nombre de données en circulation. Et ces informations sont extrêmement précieuses, puisqu'elles peuvent en soi renseigner sur des identités bancaires « piratables », sur la stratégie économique et commerciale d'une société, sur des éléments de propriété intellectuelles (comme les brevets), ou de la vie privée de chacun ou encore donner des indications sur les habitudes de consommation de catégories de personnes et ainsi signaler des marchés possiblement très rentables. Il est dès lors peu surprenant que ces données soient très prisées. Elles comportent une valeur intrinsèque non négligeable et recèlent une potentielle profitabilité extraordinaire.

La porte est ainsi ouverte à un important risque d'utilisation déloyale, invasive ou bien même malveillante de ces renseignements. Il ne s'agit, en revanche pas des seules hypothèses de réalisation d'un risque Cyber.

Nous appellerons cyber-risque ***l'ensemble des risques susceptibles d'apparaitre suite à l'usage d'un ou plusieurs systèmes informatiques éventuellement reliés en réseau***[1]. Ce risque émergeant amène la création de nouveaux produits d'assurance que nous allons donc étudier.

Il s'agit en effet d'un risque dont la présence, la fréquence en termes d'actes de malveillance, et la complexité s'accroissent au fur et à mesure d'avancées technologiques en accélération constante, de l'interconnexion des réseaux et maintenant des objets, de la mondialisation des échanges, avec une possibilité relativement aisée d'intrusion et de prise de contrôle à distance. L'entreprise, comme le citoyen, ou les organes de l'État sont aujourd'hui de plus en plus dépendants de la sécurité, des performances et de l'efficacité de leur système informatique, et des réseaux connectés.

Toutefois, les très grandes entreprises et sociétés de notoriété internationale ne sont pas les seules visées par les attaques malveillantes de pirates informatiques. [2]En décembre 2015, 52,4%

[1] AIG, Conférence sur la cyberassurance, Paris, Mars 2017
[2] Haude-Marie THOMAS. « Dossier : Le risque Cyber ». Argus de l'assurance 1er Juillet 2016

des attaques ciblées touchaient des Petites et Moyennes Entreprises (PME). Face à de tels résultats on comprend aisément que ce sont toutes les entreprises qui peuvent être visées par des attaques numériques indépendamment de leur taille. Cependant les conséquences de telles atteintes aux systèmes informatisés ne sont pas les mêmes, suivant la dimension de l'entreprise ou de l'entité ciblées. En effet les petites structures n'ont pas toujours les fonds nécessaires au rétablissement de leur dispositif, ou à la prise en charge des coûts supplémentaires engendrés par l'attaque ni les pertes qu'elle a pu occasionner.

La première ligne de défense des entreprises contre les cybermenaces est constituée par des investissements accrus dans la technologie de sécurité et des pratiques des gestions de risque robuste et complètes. Bien des entreprises recherchent aussi des solutions externes pour gérer leurs cyber expositions y compris le transfert des risques à des parties tierces mieux à même de les absorber. Un marché dédié à la cyberassurance se développe rapidement, si bien que le nombre d'acteurs désireux de souscrire d'avantage d'affaires dans cette branche de spécialité augmente. Mais certains cyber-risques importants restent largement non assurés. Et l'ampleur de la couverture est modeste par rapport aux expositions globales des entreprises

Le marché de la cyberassurance est en construction et ses produits en phase d'ajustement. Alors qu'il jouit d'une croissance soutenue, il se heurte cependant à la méconnaissance d'un risque récent et évolutif et au potentiel de cyber-catastrophistes qui freinent l'offre de réassurance. Gestion du risque par les assurés, environnement réglementaire adapté et développement de l'expertise chez les assureurs et réassureurs sont les conditions pour que ce marché parvienne à maturité. Au-delà de sa seule couverture, le péril cyber est révélateur des transformations à venir dans le paysage des risques pour le marché de l'assurance et de la réassurance.

L'objectif de ce mémoire est donc de faire une synthèse des connaissances actuelles sur le produit cyber risque, c'est-à-dire, étudier avec une vision assurantielle le marché des risques cybernétiques afin de souligner tous les aspects et les prospects de ce dernier

Dans une première partie, nous allons établir un aperçu général de l'état du marché cyber à l'échelle mondiale puis à l'échelle nationale, en nous concentrant sur l'évolution des cyber risques et de la cyberassurance en parallèle.

La deuxième partie va porter principalement sur la conception et la création d'un produit assurance des risques cyber adapté aux besoins de marché national à travers une étude de

marché basée sur une enquête dont la cible est le secteur bancaire comme un départ qui peut être généralisé après pour d'autres secteurs.

CHAPITRE I : ASSURABILITÉ DES RISQUES CYBERNÉTIQUES

CHAPITRE I : ASSURABILITÉ DES RISQUES CYBERNÉTIQUES

INTRODUCTION :

Par un acte de malveillance, par négligence ou simplement par erreur, il est possible d'atteindre le système d'information et les données qu'il contient. Dans ce contexte, nul doute que toutes personnes ayant la gestion ou détenant des informations numériques encourent le risque que ces dernières fassent l'objet d'atteinte pouvant affecter négativement les personnes concernées par les renseignements, dont les exemples sont déjà nombreux en pratique, dans ce premier chapitre nous allons présenter le vocabulaire technique et le marché des risques cyber, ainsi l'évolution de la demande de la cyberassurance, terminerons avec un aperçu sur le marché algérien.

SECTION 1 : ÉVOLUTION DES RISQUES CYBERNÉTIQUES DANS LE MONDE

Le premier gros incident cyber mondial répertorié a eu lieu en 1988[1] : loin d'être une attaque cyber orchestrée, cet incident n'était même pas intentionnel. Ce dernier a été provoqué par Robert Morris, un étudiant âgé de 23 ans, qui décida de créer un programme permettant de connaître le nombre d'ordinateurs connectés à Internet. Il a ainsi, par erreur, propagé un ver informatique qui a saturé la mémoire vive de 5 % de l'ensemble des ordinateurs connectés à Internet à l'époque. Cet incident a permis la mise en place des premiers groupes dédiés à la protection à la fois technique et légale des données et de la confidentialité.

1 - DÉFINITION :

Le cabinet français de courtage en assurance définit les Cyber-risques comme « ***les conséquences d'une atteinte aux données numériques détenues et/ou gérées par l'entreprises, que celles-ci lui appartiennent ou qu'elles lui soient confiées par les tiers, ainsi que les conséquences d'une atteinte aux systèmes informatiques***[2] ». Cette définition simple embrasse néanmoins un large champ de situations qui peuvent survenir chaque jour dans la pratique professionnelle. Mais alors, pourquoi évoquer sérieusement le risque Cyber peut-il se révéler être une tâche plus difficile qu'il n'y paraît ? L'une des raisons est avant tout liée à

[1] Baromètre de la cybersécurité des entreprises », Cesin - Opinion Way, janvier 2019
[2] « Americans and Cybersecurity » Pew Research Center, January 26, 2017).

l'imaginaire collectif qu'il suscite. En effet, le terme de « risque Cyber » semble digne d'un scénario de science-fiction et pourtant la réalité est tout autre.

Cependant il est nécessaire pour concevoir vraisemblablement ce risque de lier des notions quotidiennes (comme l'utilisation de matériel informatique, de service bancaire ou de l'internet) avec des concepts beaucoup plus flous et éloignés de nos préoccupations habituelles. En outre, les grands scandales en la matière dont fait état la presse, rendent encore plus surréaliste la notion de risque Cyber. On peut par exemple évoquer le vol de données relatifs à 77 millions de clients qu'avait subi l'entreprise Sony en 2011 ainsi que l'indisponibilité de ses services provoquant alors une perte de chiffre d'affaire annuel d'environ 450 million d'euro[1] .

Toutefois, les très grandes entreprises et sociétés de notoriété internationale ne sont pas les seules visées par les attaques malveillantes de « pirates informatiques ». Le Global Intelligence Network de Symantec, qui est un réseau mondial d'observation des menaces informatiques révélait qu'en décembre 2015, 52,4 % des attaques ciblées touchaient des Petites et Moyennes Entreprises (PME). Face à de tels résultats on comprend aisément que ce sont toutes les entreprises qui peuvent être visées par des attaques numériques indépendamment de leur taille. Cependant les conséquences de telles atteintes aux systèmes informatisés ne sont pas les mêmes, suivant la dimension de l'entreprise ou de l'entité ciblées.

De surcroit, une étude menée par The Global State of Information Security Survey 2016, nous apprend ainsi que le nombre de Cyber attaques recensées a progressé de 51% en France en 2015.

Si le Cyber risque évoque en premier lieu les actes de piratage ou de vols informatiques, ces actes de malveillance ne sont pas les seules qui peuvent causer des atteintes aux données numériques. Ainsi, les erreurs humaines dans la programmation, l'installation et le développement des activités numériques peuvent être à l'origine de dégradations, de pertes ou de diffusion de toutes sortes de données traitées, stockées ou gérées par une entité, ce qui peut alors produire des effets négatifs sur les personnes concernées par les informations endommagées. À noter également que la moitié des attaques sont favorisées par la négligence humaine[2].

[1]Haude-Marie THOMAS. « Dossier : Le risque Cyber ». Argus de l'assurance 1er Juillet 2016
[2]Haude-Marie THOMAS. « Dossier : Le risque Cyber ». l'Argus de l'Assurance du 1er Juillet 20

Outre les données bancaires, les données relatives à la propriété intellectuelle, ou à la stratégie économique et commerciale d'une entreprise, les données à caractère personnelles font également l'objet de beaucoup d'attention, tant de la part des acteurs économiques que des politiques. Il s'agit de données qui appartiennent à des personnes tierces à l'entité qui les traitent c'est-à-dire aux clients, aux collaborateurs, à des fournisseurs ou des partenaires. En effet, ces données peuvent représenter une très grande valeur monétaire parce qu'elles renseignent sur les pratiques des personnes, les habitudes de consommation, les loisirs, les activités, la profession, et les données bancaires, tant d'informations qui retranscrites en termes de consommation peuvent indiquer des marchés potentiellement très profitables.

Les données bancaires parce qu'elles permettent d'atteindre directement ou indirectement des comptes bancaires et de s'approprier les sommes qu'ils contiennent demeurent en enjeux crucial. Les conséquences d'une atteinte aux données bancaires peuvent s'avérer redoutables tant pour l'entité qui traite ces données que pour les propriétaires victimes de l'atteinte. Outre les pertes financières pures, il s'agit aussi de l'impact en termes d'images pour les personnes chargées de la gestion des données bancaires. En effet la perte de confiance et les nuisances engendrées à la réputation de la personne responsable du traitement de données qui subit un cyber attaque peuvent mettre fin à son activité, voir à son existence pour les personnes morales.

Les exemples parlent d'eux-mêmes, le 7 septembre 2017, la société Equifax, l'une des plus importantes agences de crédit américaines, qui collecte et analyse les données personnelles de consommateurs sollicitant un prêt, a annoncé que son système informatique avait été piraté. En jeu, la fuite potentielle des données sensibles de pas moins de 143 millions d'Américains : noms, adresses, numéros de cartes de crédit ou de Sécurité sociale. Même chose pour 57 millions d'utilisateurs d'Uber. En Europe, toujours en 2017, les hôpitaux britanniques, le fournisseur de télécoms espagnol Telefónica, Saint Gobain, le ministère russe de l'Intérieur ou la Deutsche Bahn, parmi beaucoup d'autres, ont été ciblés par les logiciels de ransomware « WannaCry[1] » et « Petya [2]».

[1]Wannacrypt un logiciel malveillant utilisé lors d'une attaque massive touchant plus de 300 000 ordinateurs dans plus de 150 pays.

[2] Logiciel malveillant de type rançongiciel il chiffre la table de fichier pricipale.

Tableau n° (I.01) : Liste des attaques cybernétiques les plus couteuses entre 2017-2019.

DATE	CYBERATTAQUE	PAYS/REGION	PERTES	HACKER
12/05/2017	Wannacry	Monde	4-8 milliards USD	Inconnu
27/06/2017	NotPetya	Monde	10 milliards USD	Inconnu
21/02/2019	Attaques informatiques massives	Monde	5 milliards USD	Inconnu
Juillet 2019	Vol des données de la banque Américaine Capital ONE	Etats Unis Et Canada	Vol de données personnelles de 106 millions de clients de la banque	Inconnu
Juin 2019	Attaque informatique d'Eurofins	France	70 millions USD	Inconnu
15/07/2020	Twitter	Etats Unis	12.85 BTC Soit +500K USD	

Source : **ATLAS MAGAZINE**

La plupart des cybercriminels sont encore inconnus des autorités. Même si un groupe de hackers prétend avoir commis un crime, ils sont rarement poursuivis, car ces groupes sont généralement composés de plusieurs membres et leur identité est difficile à identifier.

2 - L'ÉVOLUTION DES RISQUES CYBERNÉTIQUES DANS LE MONDE

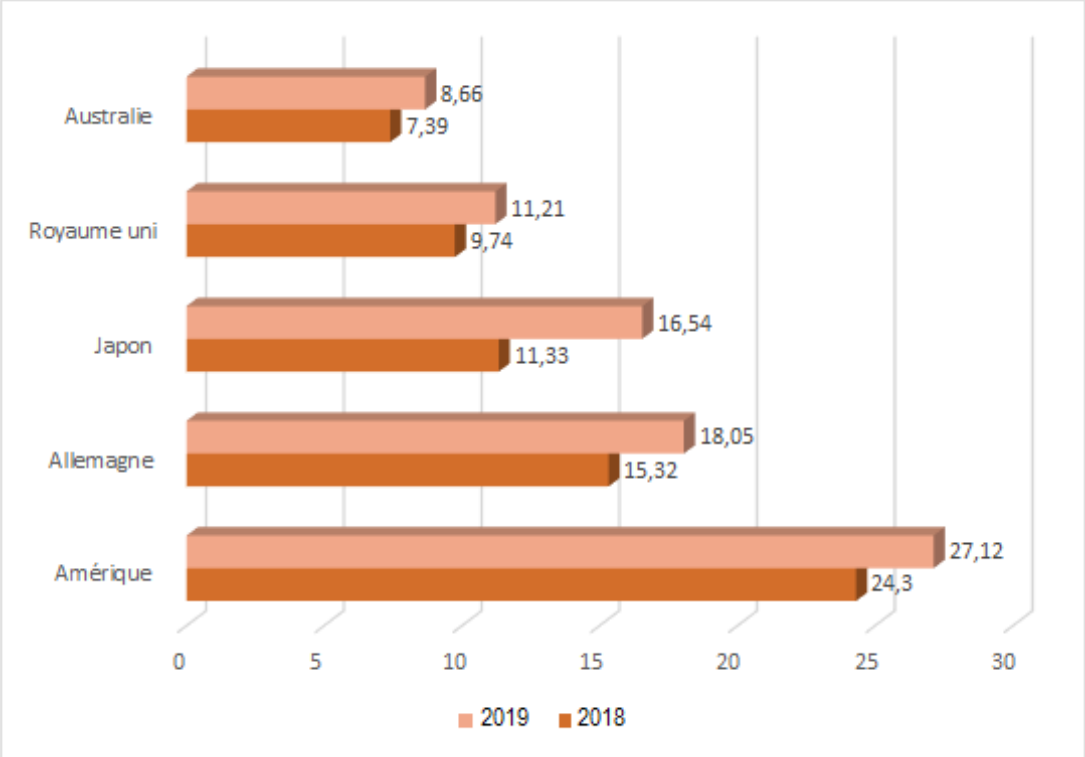
En 2017, ce n'était pas moins de 978 millions d'utilisateurs dans le monde qui ont subis une attaque cyber ainsi que 172 milliards de dollars dérobés (Symantec : Norton Cyber Security Insights Report 2017).

D'autre part, 61% des grandes entreprises ont été cibles d'une ou de plusieurs cyber-attaques au cours de l'année 2018. Le coût moyen d'un cyber incident augmente d'année en année. Il se situe entre 200 000 USD et 1,3 million USD pour les petites et moyennes entreprises et peut atteindre jusqu'à 27 millions USD pour les grandes entreprises américaines.

2.1 - Par région :

La plateforme Statista[1], a publié novembre 2017 le coût estimé des crimes cybernétiques en millions de dollars sur un échantillon de 254 compagnies différentes entre les années 2018 et 2019. La figure ci-après montre les résultats pour cinq pays / régions différents

Figure n° (I.01) : Évolution du coût des attaques cybernétiques en millions de dollars entre 2018 et 2019



Source : http://www.statista.com/

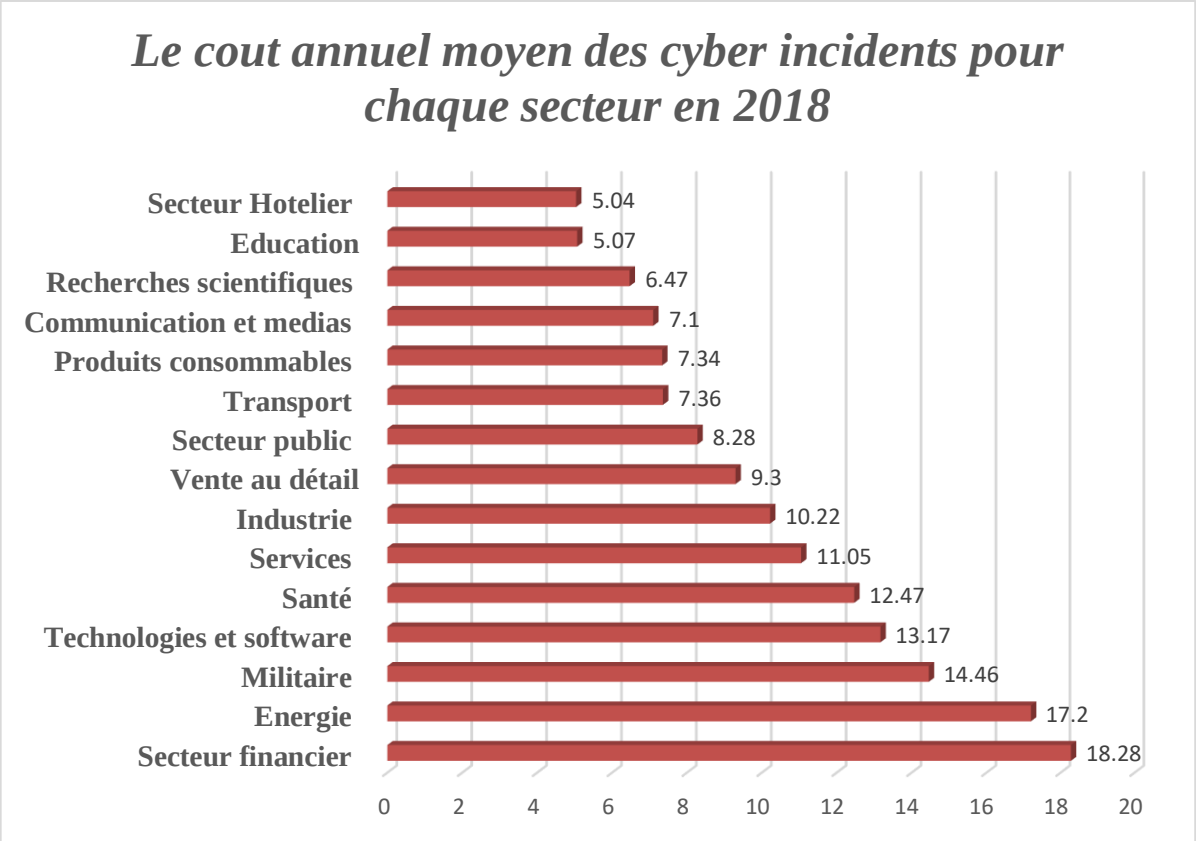
Les entreprises américaines ont le coût le plus élevé avec une évolution de 22%, tandis que l'Australie a le coût le plus bas avec une évolution de 7%. Le pays avec l'évolution la plus importante est le Japon, avec 46%.

[1] Statista : un portail en ligne allemand offrant des statistiques issues des données d'instituts, d'études de marché et d'opinion ainsi que des données provenant du secteur économique

2.2 - Par secteur d'activité :

Dans ce cas, la classification est basée sur 15 secteurs différents. Comme le montre le graphique ci-dessous, les secteurs financiers et énergétiques ont les coûts annuels moyens de la cybercriminalité les plus élevés, alors que les compagnies d'éducation et le secteur hôtelier représentent le coût le plus faible.

Figure n° (I.02) : le cout moyen des cyber incidents pour chaque secteur en 2018



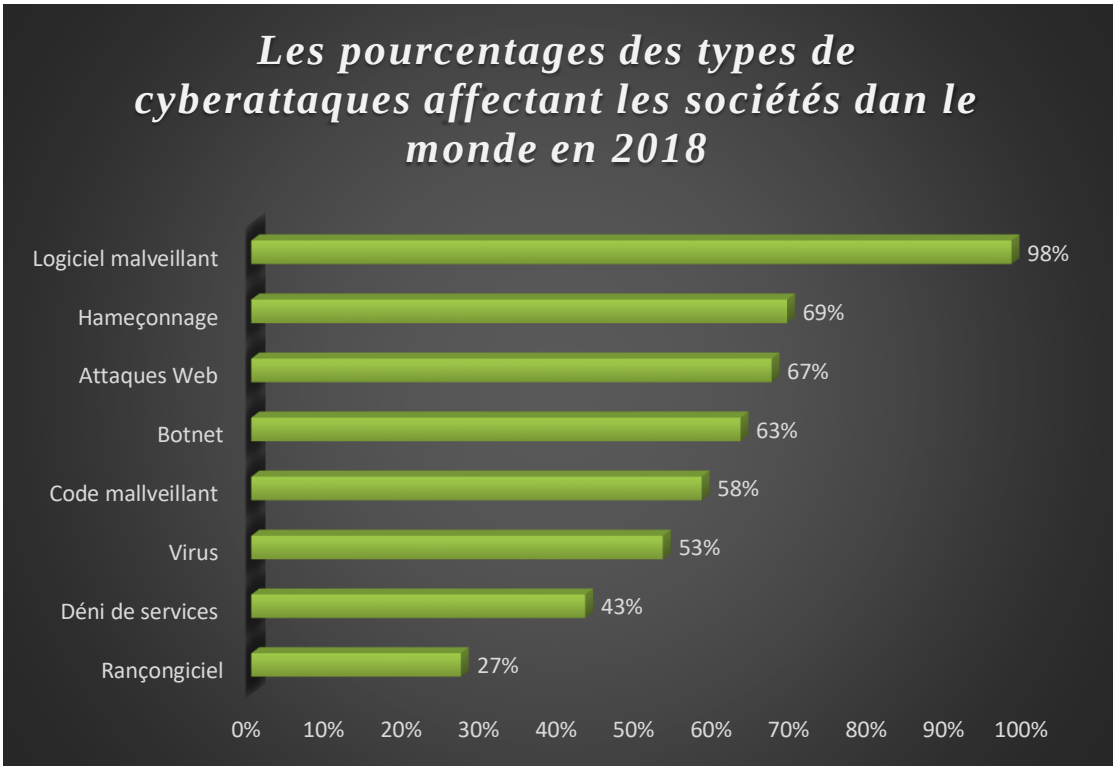
Source : http://www.statista.com/

2.3 - Par type d'attaque

Comme le montre la figure3, ci-dessous, les entreprises dépensent respectivement un coût moyen de $2.4 millions et de $2 millions pour les pertes causées par les attaques de type logiciels malveillants et attaques web. En contrepartie les attaques les moins coûteuses sont celles causées par les rançongiciels et les botnets[1] pour des coûts respectifs de $532,914 et $350,012 milles.

[1]Botnet est un terme générique qui désigne un groupe d'ordinateurs infectés et contrôlés par un pirate à distance

Figure n° (I.03) : Pourcentage de chaque type d'attaque cybernétique dans le monde



Source : www.statista.com

3 - CATÉGORISATION DES RISQUES CYBERNÉTIQUES [1]

Le cyber-risque peut être classifié selon le type d'activité (ex : criminel et non criminel), selon le type d'attaque (ex : logiciel malveillant) ou encore la source (ex : terroriste, criminels et gouvernements), il peut provenir des sources en dehors de l'organisation, tels que les cybercriminels ou bien des sources internes à l'organisation telle que les employés ou les entrepreneurs. La combinaison de ces deux dimensions nous conduit à l'inventaire et la catégorisation des risques cybernétiques de la sorte :

- ***Internes malveillants*** : Actes délibérés de sabotage, de vol ou d'autres méfaits commis par une ou plusieurs personnes internes à l'organisation. Par exemple, un employé mécontent se procède à supprimer des informations clés avant de quitter l'organisation ;

- ***Internes non intentionnels*** : Actes entraînant des dommages ou des pertes découlant d'une erreur humaine commise par des employés. Par exemple, en 2013, le NASDAQ

[1]Haude-Marie THOMAS. « Dossier : Le risque Cyber ». L'Argus de l'Assurance du 1er Juillet 20

(c'est le deuxième plus important marché d'actions des États-Unis) a connu des difficultés dans le système d'information interne qui ont entraîné l'échec des systèmes de sauvegarde ;

- ***Externes malveillants*** : c'est le risque cybernétique le plus médiatisé, il s'agit des attaques préméditées de la part d'un tiers (piratage, vol d'informations, harcèlement, escroquerie…). Les exemples incluent l'infiltration du réseau et l'extraction de la propriété intellectuelle ainsi que le déni de service (DDoS : Distributed Denial of Service) ce sont les attaques qui causent des problèmes de disponibilité du système, des interruptions d'activité, et affectent la performance des dispositifs connectés tels que des dispositifs médicaux ou des systèmes industriels ;

- ***Externes Non-intentionnels*** : Semblable au non-intentionnel interne, ceux-ci causent la perte ou les dommages aux affaires, mais ne sont pas délibérés. Par exemple, un partenaire tiers confronté à des problèmes techniques peut avoir un impact sur la disponibilité du système, tout comme les catastrophes naturelles.

Ces différentes catégorisations du risque mettent l'accent sur les activités criminelles, mais il est évident que les activités non criminelles constituent une part importante des éléments constituants du cyber-risque.

4 - PRÉVENIR LES RISQUES CYBERNÉTIQUES

➢ *L'hameçonnage et le harponnage*[1]

L'hameçonnage (ou « phishing » en anglais) et le harponnage (ou « spear-phishing » en anglais) consistent à dérober des données personnelles (mots de passe, identifiants bancaires…) en apaisant la méfiance de la victime.

Pour y parvenir, les pirates se font passer pour des tiers de confiance dont la légitimité n'est pas discutable : administration, banque, assurance, opérateur téléphonique, fournisseur d'énergie…

[1]Baro mètre de la cybersécurité des entreprises », Cesin - Opinion Way, janvier 2019.

Un exemple de tentative d'hameçonnage : Un salarié d'une entreprise de logistique reçoit un mail d'un expéditeur qu'il croit être son fournisseur. Il ouvre la pièce jointe, porteuse d'un programme malveillant. Le système d'information, dont certains logiciels n'ont pas été mis à jour, se trouve paralysé. La société ne peut plus assurer les livraisons de marchandises de ses clients. Il est nécessaire de faire appel à des prestataires extérieurs et de réutiliser d'anciens logiciels, pour redémarrer l'activité en mode dégradé

Les bons réflexes à adopter :

- ✓ Jamais une administration ou une entreprise ne demande d'informations personnelles sensibles par courriel, SMS ou téléphone. Si cela arrive, il ne faut surtout pas les communiquer et contacter directement l'organisme concerné (sans utiliser les coordonnées fournies dans le courriel ou le SMS douteux) ;

- ✓ Si le courriel renvoie vers un site internet dont vous doutez de l'authenticité, aucune opération ne doit être effectuée sans avoir vérifié que l'adresse Internet est conforme à celle consultée habituellement.

- ➢ ***La fraude informatique*** :

Elle consiste le plus souvent à usurper l'identité d'une personne de confiance après une utilisation non autorisée d'un système d'information, afin d'obtenir le versement d'une somme d'argent importante. Pour préparer leur attaque, les malfaiteurs :

- Lancent une campagne de harponnage[1], pour récupérer des identifiants ou installer un programme malveillant qui permettra de s'introduire dans le système informatique de l'entreprise ;
- Étudient la société et son fonctionnement à travers son organigramme, ses partenaires ou encore l'emploi du temps du dirigeant ;

Un exemple de fraude informatique : Une société du secteur pétrolier est avertie par son expert-comptable d'un mouvement bancaire suspect. Elle constate en effet un virement depuis sa banque vers un compte qu'elle ne connaît pas, un nouveau bénéficiaire ayant donc été créé à son insu, suivi d'un virement. Après investigations, il s'avère que des hackers ont trompé l'une des personnes de cette société en lui envoyant un mail frauduleux. Cette personne, en

[1]Harponnage (ou « spear-phishing » en anglais) : une déclinaison de l'hameçonnage, qui s'appuie sur une connaissance de la cible et une pe rsonnalisation du message

ouvrant la pièce jointe du courriel, a ainsi permis l'installation d'un logiciel malveillant sur son poste informatique, permettant l'accès non autorisé au système d'information de l'assuré. Les pirates ont alors pu saisir un ordre de virement du compte bancaire de la société vers leur compte.

Les bons réflexes à adopter :

- ✓ Sensibilisez les salariés en leur présentant la mécanique de ce type de fraude ainsi qu'aux techniques d'hameçonnage[1] et de harponnage.
  En cas de mail douteux, saisissez vous-même l'adresse de votre destinataire, plutôt que de faire « répondre à » ;
- ✓ Assurez la confidentialité des organigrammes (et a minima, en extraire le nom et les coordonnées des responsables financiers et comptables) ;
- ✓ Prévoyez un protocole de double signature pour tout virement supérieur à une certaine somme ;

➢ ***Les rançongiciels*** :

Sont un type particulier de logiciel malveillant qui, une fois installé sur une machine, chiffre les données qu'elle abrite pour les rendre inaccessibles. Une demande de rançon sera alors adressée à la victime par le pirate, en échange d'un code permettant de « libérer » les informations retenues en otage.

Un exemple d'attaque par un rançongiciel : Un aéroport britannique fait l'objet d'une attaque d'un rançongiciel. Pendant deux jours, les écrans d'affichage en temps réel sont hors service, pour limiter la propagation des dommages et réparer le SI. Le personnel doit recourir à des tableaux blancs pour informer les voyageurs sur le statut de leurs vols.

Les bons réflexes à adopter :

- ✓ Mettre régulièrement à jour les systèmes d'exploitation, l'antivirus et les pare-feu[2] ;
- ✓ Ne jamais ouvrir des courriels dont la provenance ou la forme est douteuse ;
- ✓ Interdire l'installation de logiciel sans l'accord de la DSI ;

[1]Hameçonnage (ou « phishing » en anglais) : technique qui consiste, pour les pirates informatiques, à envoyer un mail aux couleurs d'un partenaire ou d'un prestataire de confiance, dans le but de dérober des informations.

[2]Pare-feu (ou « firewall » en anglais) : outil permettant de protéger les ordinateurs connectés à un réseau. Il protège d'attaques externes (filtrage entrant) et souvent de connexions illégitimes à destination de l'extérieur (filtrage sortant)

- ✓ Effectuer des sauvegardes régulières des données de l'entreprise sur des supports non connectés en permanence aux machines. En cas d'attaque, vous pourrez ainsi effectuer un formatage et réinstaller les données.

SECTION 2 : ASSURANCE DES RISQUES CYBERNÉTIQUES

1 - LE MARCHÉ D'ASSURANCE CYBERNÉTIQUE

De petite taille, le marché de l'assurance cyber est détenu, pour l'heure, par des assureurs extrêmement prudents. Ces derniers font face à un risque difficile à appréhender, évolutif et très coûteux. De plus, l'absence d'historique sinistre peut déboucher sur une prime totalement inadaptée.

Malgré ces obstacles, la cyberassurance se développe à un rythme soutenu. Selon les données de Munich Re, le marché est évalué à 3,5 milliards USD à fin 2018. Concentré aux Etats-Unis, la cyberassurance va doubler son chiffre d'affaires d'ici 2020 et atteindre, toujours selon le réassureur allemand, 20 milliards USD de primes à l'horizon 2025.

Face à la complexité du risque, des solutions sont de plus en plus développées par les grands opérateurs du marché. Chubb[1] et AXA couvrent, à eux deux, plus de 30% des cyber-risques du marché américain. Trust Insurance Management, société de gestion de risques basée à Bahreïn, s'est également lancé dans la souscription des couvertures cyber auprès des entreprises des pays du Conseil de Coopération du Golfe.

À ce jour, la sinistralité engendrée par ce risque a été bien gérée par le marché. Une hausse des taux de prime des contrats cyber a été enregistrée depuis les attaques WannaCry et NotPetya. Dans l'ensemble, les taux ont connu une hausse de plus de 50% en 2019[2].

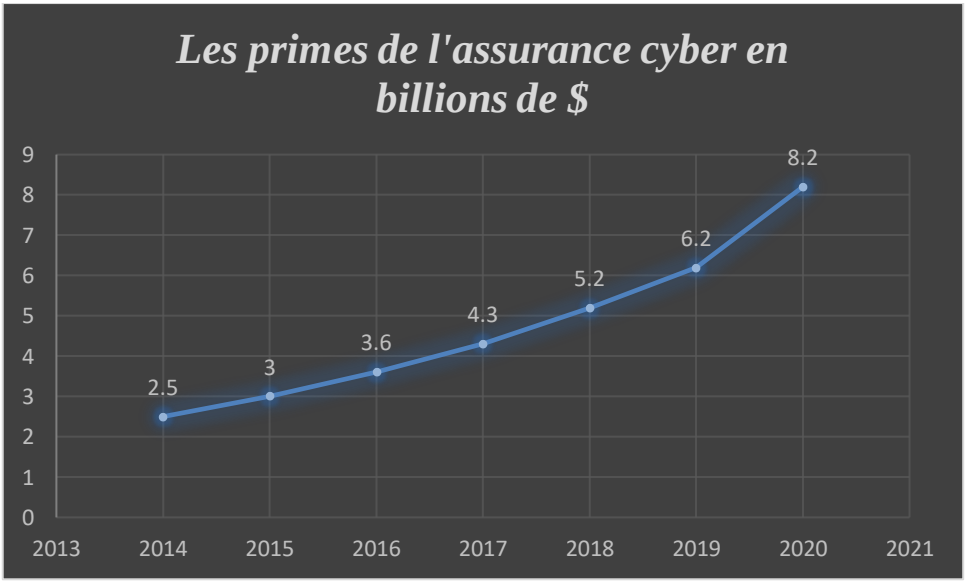
L'Amérique du Nord - et particulièrement les États-Unis, qui détenaient 90 % des primes en 2014 - domine le marché de la cyber assurance, juste devant l'Europe. La part de marché de la zone Asie-Pacifique reste limitée, les primes cumulées dans la région s'élevant à 50 millions de dollars en 2017[3]. Ce chiffre concernant l'assurance des entreprises devrait augmenter significativement dans les années à venir. Cette évolution est due à plusieurs facteurs :

[1] Chubb limited, anciennement ACE limited est un consortium d'assurance et de réassurance issu de regroupement de 34 société.
[2] https://www.atlas-mag.net/article/le-marche-de-la-cyberassurance-en-2019
[3] https://techwireasia.com/2019/02/why-cyber-insurance-market-set-to-surge-in-the-apac/

- Les lois et les régulations veillant à la protection des personnes et des organisations contre la violation des données est particulièrement accrue en Amérique ;
- Le nombre important des incidents cybernétiques qui ont touché plusieurs organisations reconnues en Amérique (exemple : Sony en 2001, Target en 2014, EBay en 2014, Yahoo en 2013 et 2014... etc.) ont contribué à attirer l'attention et à éveiller la conscience du public d'une part et des autorités de régulation et d'exécution d'autre part concernant la gravité des menaces des risques cybernétiques ;
- Le risque cybernétique est classé 2ème en termes d'importance et de gravité en 2017 alors qu'il était 18 -ème en 2011.

L'évolution de niveau des primes cybernétiques dans le monde se présenter par la figure suivante :

Figure n° (I.04) : L'évolution des primes d'assurance cyber dans le monde de 2014 à 2020



Source : www.statista.com

Une évolution qualifiée d'exponentielle avec un volume de primes qui atteint 6.2bn USD en 2019 et qui est estimé atteindre 8.2bn USD en 2020.

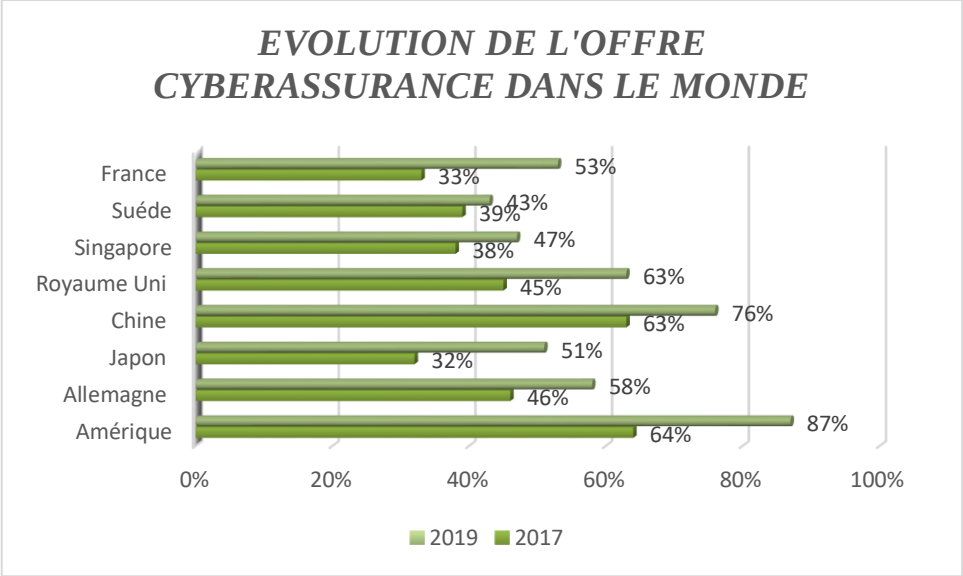
2 - L'ÉVOLUTION DE L'OFFRE CYBER ASSURANCE

Ces dernières années, en particulier après les attaques contre Wannacry et Notpetya, que de nombreuses entreprises et administrations ont estimé nécessaire l'instauration de nouveaux

protocoles de sécurité, la demande de cyberassurance a donc augmenté, ce qui signifie que davantage de cyber assurance est fournie.

La figure suivante montre cette évolution de 2017 à 2019. Les États-Unis est le grand fournisseur de ce produit, avec une proportion de 87% en 2019.

Figure n° (I.05) : L'évolution de l'offre cyber assurance dans le monde de 2017 à 2019



Source : www.statista.com

Les conséquences dommageables consécutives à des faits générateurs cyber, accidentels ou malveillants ne sont que partiellement couvertes par les contrats traditionnels existants, qui n'ont pas été conçus pour une économie largement numérique comme celle que nous connaissons aujourd'hui. De nouveaux contrats dédiés spécifiquement aux risques cyber ont donc été progressivement développés pour couvrir les conséquences dommageables qui ne sont pas nécessairement prises en charge par les contrats traditionnels.

2.1 - Un risque partiellement couvert par les contrats traditionnels

Avant que des contrats spécifiques ne se développent, de nombreuses conséquences dommageables d'un cyber-risque étaient déjà couvertes par les contrats d'assurance traditionnels[1]

[1] Philippe MALAURIE, Laurent AYNES, Philippe STOFFEL-MUNK. « Droit des obligations ». 7ème Edition. LGDJ, Lextenso édition. 2016

A - Les contrats de dommages aux biens

Les faits générateurs cyber, qu'ils soient d'origine malveillante ou issus d'erreurs humaines, peuvent engendrer des conséquences dommageables matérielles. Elles seront couvertes par le contrat dommages aux biens. Avec ce contrat, les dommages physiques aux biens de l'assuré et les pertes d'exploitation consécutives seront couverts quel que soit le fait générateur cyber. À contrario, si le fait générateur cyber ne crée pas de dommage matériel, les pertes d'exploitation ne peuvent être couvertes par ce contrat.

B - Les contrats de responsabilité civile

Par nature, les contrats de responsabilité civile couvrent les dommages corporels, matériels et immatériels causés aux tiers, quel que soit leur fait générateur. Ils couvrent également les frais de défense et de recours de l'assuré lorsque ce dernier est la victime. Par conséquent, les sinistres de responsabilité civile résultant d'un fait générateur cyber d'origine malveillante ou consécutifs à une erreur humaine seront couverts par ces contrats. Par exemple, un responsable de traitement de données à caractère personnel mis en cause pour atteinte à la vie privée à la suite d'une violation puis d'une divulgation de données à caractère personnel consécutive à un acte de malveillance ou à un accident pourra être couvert par son contrat de responsabilité civile.

Il en va de même pour une entreprise victime d'une cyberattaque qui la contraint à arrêter sa production et à suspendre ses livraisons. Par manque d'approvisionnement, ses propres clients peuvent également être amenés à arrêter leur production. Ils subissent alors un préjudice dont l'entreprise victime de l'attaque cyber pourra être tenue responsable. Ces préjudices pourront être couverts par le contrat de responsabilité civile de l'entreprise victime de la cyberattaque.

C - Le contrat Fraude

Les contrats Fraude existent de longue date. Ils couvrent les actes frauduleux tels que le détournement de fonds, l'escroquerie, le faux ou l'usage de faux, la contrefaçon et le vol. Les conséquences dommageables d'une fraude assistée par ordinateur sont couvertes par les contrats Fraude et non pas par les contrats cyber. À titre d'exemple, les faux ordres de virement par usurpation d'identité (fraude au président) restent du périmètre exclusif des contrats Fraude, même s'ils utilisent des nouvelles technologies (faux e-mails, usurpations d'identité numérique…). Lorsque la fraude est facilitée par l'introduction d'un logiciel malveillant dans le système informatique, les conséquences dommageables de ce seul fait générateur pourront être couvertes soit par les contrats Fraude soit par les contrats cyber.

2.2 - Le développement de contrats spécifiques

L'émergence de nouveaux risques liés à l'évolution des nouvelles technologies de l'information et de la communication et à l'accroissement de leurs usages a nécessité et nécessite encore la mise en place de cadres juridiques adaptés. Ainsi, en France, la loi informatique et libertés de 1978 consolidée[1] et celle de programmation militaire pour la période 2014/2019[2] ont introduit de nouvelles obligations pour les entreprises, dont l'exécution ou le non-respect induit de nouveaux frais qui ne sont pas pris en charge par les contrats traditionnels (ex. : obligation de notification, enquête administrative). Ces nouveaux risques ont entraîné l'apparition d'un nouveau type de dommages, comme les atteintes aux données personnelles des tiers et de l'entreprise, ou les pertes d'exploitation consécutives, qui ne sont pas prises en charge par les contrats traditionnels. Pour faire face à ces nouveaux risques, de nouveaux services ont été développés par les assureurs, de plus en plus nombreux à nouer, à cette fin, des partenariats avec des entreprises liées au conseil et/ou à l'édition de solutions en cybersécurité. Ces services peuvent être regroupés en quatre catégories :

- Des analyses de risques ;
- Les recherches de causes,
- La gestion de crise ;
- La couverture des frais de monitoring bancaires.

Ces nouveaux besoins de garanties et de services ont conduit à la création d'un nouveau contrat : *le contrat d'assurance cyber*. Les contrats cyber sont souvent des contrats multirisques : ils offrent des couvertures de dommages (frais et pertes subis) et de responsabilité civile (dommages immatériels aux tiers), et des services de gestion de crise. Ces contrats offrent principalement les garanties suivantes :

A - Les frais et pertes subis à la suite d'une intrusion malveillante (volet dommage) :

- Les frais d'expertise informatique ;
- Les frais de gestion de l'incident et de la crise (préservation de l'image) ;
- Les frais de reconstitution des données ;
- Les frais de réparation du système infecté ;

[1]Loi relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, 18 décembre 2013, no 2013-1168, art. 22.
[2]Agence nationale de sécurité des systèmes d'information (ANSSI).

- Les pertes d'exploitation consécutives (sans dommage matériel) .

B - Les frais à la suite d'une violation de données personnelles :

- Les frais d'enquête administrative ;
- Les frais de notification.

C - Les conséquences de la responsabilité civile :

- Les dommages chez des tiers à la suite d'un défaut de sécurité chez l'assuré ;
- Les dommages chez des tiers à la suite d'un défaut de protection des données personnelles, bancaires ou de santé de tiers ;
- Les frais d'avocat ;
- Les frais de défense recours.

3 - ASSURABILITÉ DES RISQUES CYBERNÉTIQUES [1] :

Le cyber risque rencontre actuellement plusieurs problèmes d'assurabilité.

3.1 - Historique

C'est un risque récent avec peu d'historique, qui a un peu plus de 20 ans d'âge. De plus, c'est un risque qui a changé rapidement avec le développement de nouvelles utilisations des outils informatiques. Le développement d'internet a fondamentalement changé la dimension et le type de risques en permettant une action mal intentionnée depuis n'importe quel endroit dans le monde. Internet a aussi augmenté le nombre d'interconnexions entre les réseaux d'entreprises et ainsi augmenté le risque. D'autre part, le risque continue de changer avec l'arrivée des Smartphones.

Le risque est de moins en moins localisé d'un point de vue géographique. De plus, la sécurisation du matériel est particulièrement compliquée pour un appareil qui peut être volé très facilement.

Pour préserver leur image, les entreprises cachent les incidents informatiques qu'elles ont subis. Il est donc difficile d'avoir une information pour quantifier le risque. L'obligation de

[1]Master professionnel Sciences de gestion, mention finances de marché Spécialité Actuariat du CNAM, 2015.

déclaration de vol d'information aux USA peut constituer une première base de travail, même s'il doit exister des différences de risques avec le reste du monde.

3.2 - Aléa moral

Se sachant couvert, l'assuré peut réduire sa vigilance. Pour contrer ce problème, il existe deux méthodes complémentaires, l'application d'une franchise comme dans l'assurance automobile et imposer des audits du système d'information.

3.3 - Asymétrie d'information

Ce risque comporte un biais important d'anti-sélection. En effet, il est difficile pour un assureur de bien connaitre la structure du système d'information ainsi que la formation que les équipes ont reçue sur la protection des données. L'audit du système d'information est un bon moyen pour corriger ce problème, ainsi que l'application des normes.

3.4 - Inter corrélation

Un même incident de sécurité peut impacter un grand nombre d'entreprises. En effet, de nos jours, nombreuses sont les entreprises qui utilisent les mêmes logiciels qui sont en quelque sorte standards. On peut citer Windows avec MS Office. Lorsqu'une vulnérabilité existe sur un logiciel très répandu, le risque qu'une action malveillante soit menée à bien augmente sur toutes les entreprises utilisant ce logiciel. Les cyber-risques de toutes ces entreprises sont alors corrélés.

De plus, une compromission peut avoir des conséquences sur des entreprises indépendantes. Par exemple, de nombreux utilisateurs utilisent très peu de combinaisons login/mot de passe sur internet. On retrouve donc la même combinaison sur de nombreux services pour un seul utilisateur. L'hacker qui a compromis un site peut alors usurper l'identité de nombreux utilisateurs sur d'autres sites. Il peut aussi utiliser ces informations pour faire du « fishing » ciblé, qui aura alors plus de crédibilité auprès de l'utilisateur qui se fera alors hameçonner et donnera des informations sensibles à l'hacker.

De nombreuses entreprises mutualisent les coûts en utilisant les mêmes plateformes. Il y a donc une forte corrélation entre les risques. Par conséquent les réassureurs ne veulent pas assurer ce type de risque.

4 - DIFFICULTÉ DE LA TARIFICATION DES RISQUES CYBER

Bien que les risques cyber présentent pour les assureurs des opportunités considérables, ces derniers sont confrontés à une réalité dure : La quantification précise du cyber risque sous-jacent et des impacts des failles de sécurité est exceptionnellement complexe. Les assureurs doivent développer de meilleures méthodes de modélisation du risque cybernétique pour améliorer la précision et la cohérence des tarifs proposés.

4.1 - Défis de prix [1]

Pour fixer un prix, les assureurs doivent quantifier avec précision les risques auxquels leurs clients sont exposés. Au-delà, les comparaisons avec les prix de risque conventionnels sont difficiles. Le risque cybernétique survient dans un écosystème complexe de vulnérabilités interdépendantes, de menaces à la sécurité et d'impacts potentiels associés. Il dépend également de plusieurs caractéristiques telles que :

- L'attractivité d'une entreprise en tant que cyber cible ;
- Les dommages financiers et l'atteinte à la réputation qu'une attaque cyber pourrait infliger ;
- Le système de sécurité de l'organisation, c'est-à-dire à quel point ils sont équipés pour détecter et repousser les menaces cybernétiques, en fonction de leur infrastructure et de leurs pratiques de sécurité de l'information ;
- La capacité de l'organisation à répondre efficacement à une violation.

Ces variables se sont avérées difficiles à déterminer. Cependant, un défi majeur auquel est confronté le domaine de la cybersécurité est la rareté des données historiques relatives aux menaces cybernétiques, aux violations réelles et aux impacts qui en résultent. Ce n'est que récemment qu'il est devenu obligatoire pour les entités violées, aux pays développés, de divulguer les détails de leurs violations de la sécurité informatique. Auparavant, les entreprises étaient réticentes à divulguer, volontairement, des violations en raison de dommages potentiels à la réputation. En plus de l'analyse des événements passés, les prix exacts de l'assurance cyber doivent également tenir compte des événements futurs. Ceci est particulièrement difficile, en raison d'un certain nombre de facteurs, notamment :

[1] https://www.finextra.com/blogposting/15278/cyber-insurance-pricing-quantifying-the-unknown-in-a-multibillion

- Un environnement des affaires en pleine évolution ;
- Évolution rapide de la technologie de l'information ;
- L'émergence de nouvelles menaces et failles ;
- La réglementation rapide et complexe.

L'effet combiné de ces défis rend difficile la tâche pour les cybers assureurs.

De plus, le risque de cyber est partagé entre les entreprises (Sous-traitants, fournisseurs...). Ce qui rend forte la corrélation des risques, cela signifie qu'une violation de l'un des composants d'un système interconnecté pourrait potentiellement compromettre l'ensemble du réseau. Historiquement, la corrélation des risques a été un facteur important qui rend le calcul des primes réalistes très difficile.

4.2 - Réactions des assureurs

Dans ce contexte de menaces cyber complexes et en rapide évolution, les assureurs ont réduit leur exposition au risque en proposant des polices sur mesure à des primes élevées. Cela a segmenté le marché du cyber assurance et a entravé la réalisation de son plein potentiel.

Des barrières élevées à l'entrée ont laissé les petites entreprises sans protection. Mais une vulnérabilité sérieuse s'étend au-delà des non-assurés, aux compagnies d'assurance elles-mêmes. Toute institution, financière surtout, est exposée à des corrélations de risques multiples et non comptabilisées. Le pire scénario est une catastrophe unique et majeure, un « événement de contagion » qui affecte un grand nombre de consommateurs. Il est possible qu'un tel événement puisse avoir des conséquences similaires à la crise financière de 2008.

Cette difficulté de tarification des offres s'explique le manque de données historiques sur les sinistres, la réticence des entreprises à partager l'information sur l'impact des cyber-attaques subies, et l'évolution rapide et continue des nouvelles technologies. De plus, les cyber-attaques n'ont pas toutes les mêmes conséquences sur les systèmes qu'elles affectent. Ces conséquences varient en fonction de la façon dont les entreprises et les particuliers utilisent leurs systèmes d'information. Au final, il n'existe pas de "modèle universel" de risque encouru. D'où la difficile tarification de ce risque très technique.

SECTION 3 : APERÇU SUR LE MARCHÉ ALGERIEN

1 - LA DIGITALISATION DANS LE SECTEUR ALGERIEN DES ASSURANCES

La digitalisation se définit comme l'art de convertir l'information analogique sous format numérique à l'aide d'appareils électroniques appropriés. Pour pouvoir être traitées par les systèmes automatisés ou informatiques, les informations analogiques doivent être converties en une suite composée d'informations logiques, cela s'appelle alors une information numérique. Il s'agit donc en d'autres termes, d'un processus de conversion de l'information dans un format numérique, c'est le procédé qui vise à transformer un objet, un outil, un processus ou un métier en un code informatique afin de le remplacer et de le rendre plus performant.

L'assurance connectée présente de nombreux avantages, pour le grand public et pour les entreprises. Aujourd'hui, les clients aspirent à la mobilité et à des échanges sans papier. Ils s'attendent à avoir des réponses rapides et à avoir accès aux informations essentielles. Ils sont à la recherche de solutions pour leur vie de tous les jours, voire une nouvelle relation avec leur assureur. Quant aux entreprises, elles ont tout l'intérêt à engager le virage de la digitalisation.[1] Parmi les points forts de l'assurance connectée, on peut citer :

- La relation client est améliorée ;
- La performance commerciale est bonifiée ;
- Les risques opérationnels et règlementaires sont maitrisés ;
- Le partage d'information est optimisé ;
- Les coûts de production et de commercialisation sont réduits ;
- La gestion des investissements est facilitée ;
- Les modes d'interactions avec les clients sont plus modernes ;
- L'identité numérique est développée ;
- L'utilisation des feuilles de papier est diminuée ;
- Les équipes sont plus autonomes.

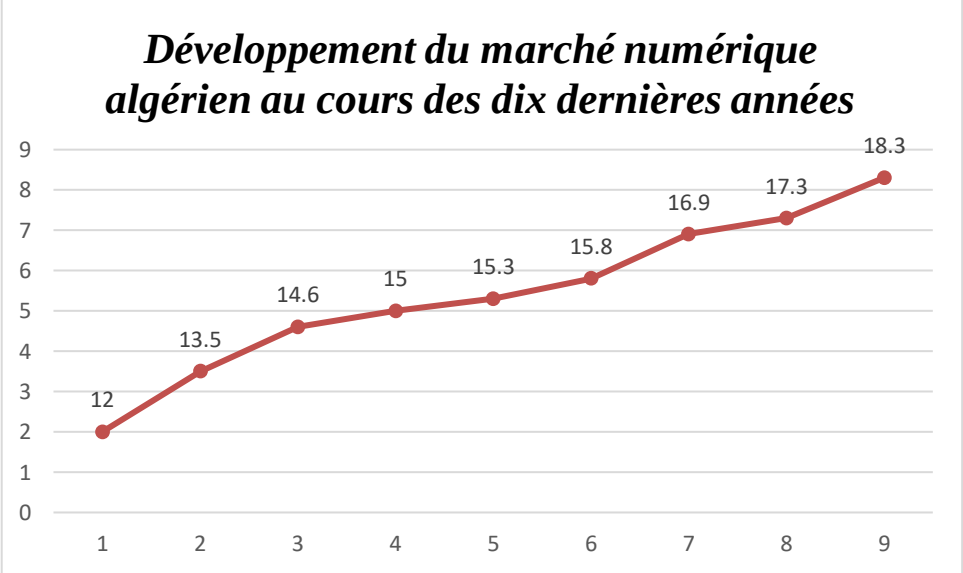
Digitaliser les processus internes c'est les généraliser et accélérer les traitements des relations extérieurs (clients, fournisseurs, partenaires) vers ceux internes, sans coupure et en

[1] Bulletin de la CCR, février 2018.

gagnant un précieux temps. Ce gain est appréciable pour l'organisation et pour la satisfaction des clients et autres partenaires extérieurs.

La solution proposée doit être une plateforme informatique globale permettant à l'entreprise, à ses clients et à ses partenaires d'y accéder via une interface simple, un environnement de travail puissant pour les collaborateurs de l'entreprise et les connecteurs nécessaires pour alimenter les autres briques du système d'information. La simplicité est facteur d'adoption et de performance.

Figure n° (I.06) : Développement du marché numérique algérien au cours des dix dernières années



Source : www.statista.com

Comme le montre la figure ci-dessus, le marché algérien a commencé à se développer en termes de digitalisation et de numérisation. Même si cette évolution est jugée modérée, c'est le début du marché numérique, le digital est désormais un allié incontournable pour développer les entreprises et s'adapter aux nouvelles évolutions de l'environnement. Les entreprises algériennes seront de plus en plus connectées, virtuelles et dématérialisées.

Le secteur de l'assurance est un secteur complexe, qui a été jusqu'à présent protégé de l'arrivée du digital dans nos vies par rapport à d'autres secteurs industriels, mais une concordance entre plusieurs facteurs technologiques, réglementaires, d'usages et d'attentes des

consommateurs va remettre le digital au cœur de tous les sujets que va connaître l'assurance au cours des prochaines années.

« Cela fait 6 ans que le risque cybernétique se positionne dans le top 5 des risques assurantiels. Aujourd'hui, le risque cybernétique est classé deuxième risque émergent après les risques de catastrophe naturelle et se situe avant les risques politiques. Ce risque est croissant de par l'augmentation du nombre d'objets connectés utilisés au quotidien.

Sur un marché mondial estimé à 2 trillions de dollars de primes, le volume des primes de risque cybernétique est de 2,5 milliards de dollars ce qui est dérisoire par rapport au potentiel réel. On estime que ce marché va, d'ici à cinq ans, tripler, mais 10 milliards de dollars restera toujours très peu, par rapport au potentiel réel, car les capacités à assurer restent limitées et inférieures à ce que l'on assure en risque incendie, par exemple. Pour pouvoir augmenter la capacité d'assurance cyber, il faut que les entreprises prennent conscience du risque cybernétique ce qui est loin d'être le cas, aujourd'hui.

Les assureurs ne prennent pas les risques de piratage informatique au sérieux. Un exemple qui illustre ce constat : les compagnies d'assurances vendent l'assurance cybernétique mais ne l'achètent pas pour protéger leurs propres systèmes[1] ».

2 - L'ÉVOLUTION DES RISQUES CYBERNÉTIQUES EN ALGERIE

Il y a une évolution importante de l'arsenal et des outils mis à la disposition des cybercriminels, toujours plus sophistiqués, ainsi que les moyens financiers conséquents dont ils disposent. Ces deux paramètres modifient les méthodes et les objectifs utilisés il y a encore quelques années.

Le graphe suivant montre l'évolution de la vulnérabilité en Algérie. La vulnérabilité est une faiblesse pour le système d'information permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient.

Selon une étude[2]publiée le 5 mai 2020, comparant 76 pays en examinant des facteurs de cyber sécurité tel que les taux d'infection aux malwares, le nombre d'attaques malwares financiers, le degré de préparation aux cybers attaques et la législation en matière de cyber

[1] Ronald Chidiac , CEO de BROKTECH SAL, Revue de L'ASSURANCE N°19 - Décembre 2017
[2] https://www.algiersherald.com/cybersecurity-in-algeria/

sécurité, l'Algérie est le pays le moins sécurisé au monde avec la législation la plus pauvre, avec seulement une loi concernant la vie privée en vigueur

L'Algérie a également obtenu de mauvais résultats pour les taux d'infection par des logiciels malveillants avec 19.75% et pour son degré de préparation aux cyberattaques de 0.262.

Figure n° (I.07) : top 10 des meilleurs et pires pays en matière de cybersécurité

Le top 10 des pays les mieux préparés Face aux cyberattaques	**Le top 10 des pires pays en matière De cybersécurité :**
1. Japon	1. Algérie
2. France	2. Indonésie
3. Canada	3. Vietnam
4. Danemark	4. Tanzanie
5. Etats-Unis	5. Ouzbékistan
6. Irlande	6. Bangladesh
7. Suède	7. Pakistan
8. Royaume-Uni	8. Biélorussie
9. Pays-Bas	9. Iran
10. Singapour	10. Ukraine

Source : Atlas Magazine

L'étude a pris en compte sept critères :

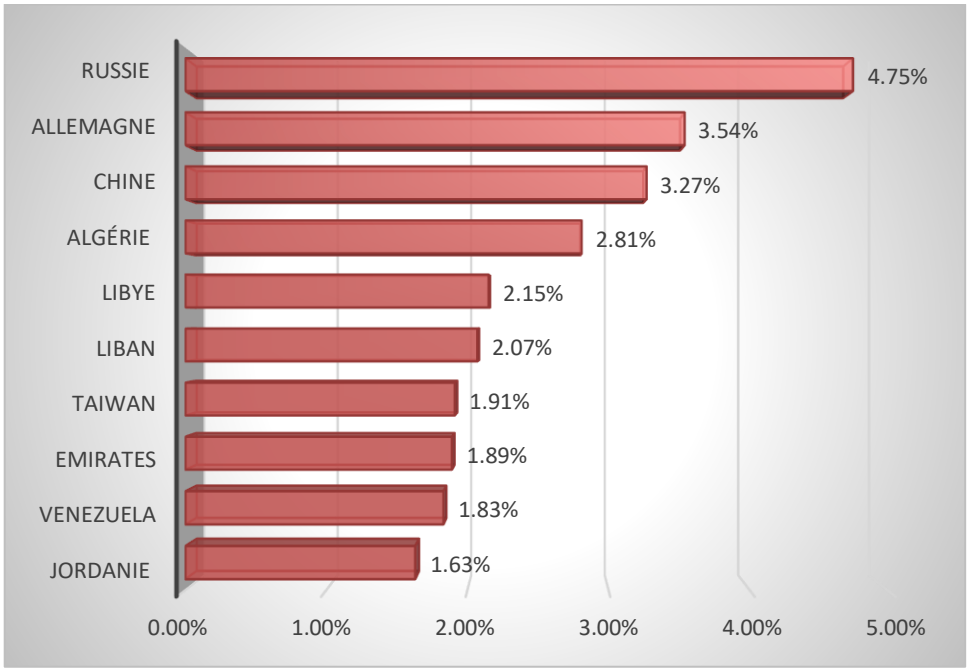
- Le pourcentage de téléphones portables infectés par des logiciels malveillants Bangladesh - 35,91% des utilisateurs ;
- Pourcentage d'ordinateurs infectés par des logiciels malveillants - Algérie - 32,41% ;
- Nombre d'attaques de logiciels malveillants financiers - Allemagne - 3% des utilisateurs ;
- Pourcentage d'attaques telnet (selon le pays d'origine) - Chine - 27,15% ;
- Attaques de sociétés cryptographiques - Ouzbékistan - 14,23% des utilisateurs ;
- Pays les moins préparés aux cyberattaques - Algérie - 0.262degrés ;
- Pire législation sur la cybersécurité - Algérie - Une catégorie principale couverte ;

De plus, la digitalisation du système bancaire qui est le pilier de la performance des banques, elle permettra de limiter les pressions sur la liquidité, lutter contre le marché parallèle, promouvoir l'inclusion financière tout en offrant des produits et des mécanismes sur mesure et une modernisation du système d'information. Mais d'un autre côté les attaques cybernétiques

vont tenter de plus en plus les cybercriminels, une seule attaque bien préparée peut générer des bénéfices énormes.

Dans la figure ci-dessous, nous pouvons voir que l'Algérie se classe quatrième parmi les banques les plus touchées au monde par les logiciels malveillants, représentant 2,81% de toutes les attaques

Figure n° (I.08) : Les banques les plus affectées par les logiciels malveillants dans le monde

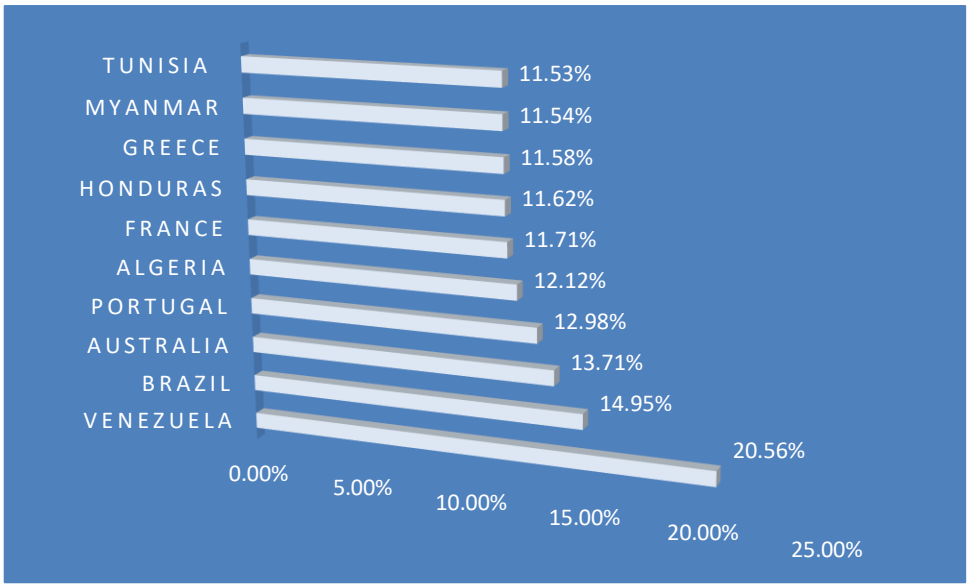


Source : www.statista.com

3 - L'ALGERIE FACE AUX CYBERCRIMINALITÉS

Selon les statistiques publiées par la plateforme Statista en 2018, l'Algérie se classe parmi les dix premiers pays souffrant du cyberterrorisme, derrière le Venezuela, Brazil et l'Australie.

Figure n° (I.09) : Les plus affectés par les cyberterrorismes dans le monde



Source : www.statista.com

Le gouvernement ne publie pas de statistiques sur cybercriminalité, et les médias et des rapports anecdotiques indiquent que la fréquence et l'intensité des activités criminelles restent modérées, de sorte que de nombreux crimes ne sont pas signalés.

Ces dernières années l'Algérie a mis soigneusement en œuvre des mécanismes juridiques pour lutter efficacement contre le cyberterrorisme, elle a coopéré avec des partenaires internationaux pour détruire et éliminer avec succès de nombreuses cellules cyberterrorismes et contenir de nombreux projets subversifs En 2015, le gouvernement algérien a officiellement mis en place une Autorité nationale de prévention et de lutte contre les violations des technologies de l'information et de la communication. Il s'agit du Centre de prévention et de contrôle de la criminalité informatique et de la cybercriminalité (CPLCIC). Selon un décret publié au Journal officiel du 8 octobre 2015, ce nouvel organe a été placé sous la responsabilité du ministère de la Justice.

L'État algérien fait face à des lacunes majeures destinées à prévenir le cyberterrorisme et à protéger les citoyens et les droits de l'homme, tels que

- La non-conformité de nombreuses structures publiques aux mesures légales et réglementaires dans ce domaine représente une menace sérieuse dont peut profiter les terroristes pour accéder aux informations confidentielles[1] ;

[1] https://www.osac.gov/Country/Algeria/Content/Detail/Report/aceef5ea-f045-453b-8fc9

- L'ajustement de la classification des données sensibles, et la sélection des informations qui peuvent être diffusées afin de limiter leur utilisation par des cyber-terroristes.

Afin de faire face aux effets désastreux du cyberterrorisme sur l'économie, les infrastructures et les niveaux social et psychologique, l'Etat algérien est appelé à adopter une approche stratégique qui implique principalement les aspects suivants[1] :

Le cadre législatif :

- Adopter un règlement régissant le monde virtuel lié aux diverses menaces causées par le cyberterrorisme, y compris la surveillance des plateformes de médias sociaux pour détecter, répondre et arrêter toute éventuelle propagande terroriste, la communication entre la radicalisation et l'utilisation dans la planification Attaques terroristes ou recrutement de personnel et autres éléments terroristes connus liés au terrorisme sur Internet, aux activités d'exploration de données et à la surveillance des activités terroristes sur le « **Dark Web**». Des mécanismes appropriés doivent être mis en place pour garantir le respect de la liberté d'expression et du droit à la vie privée. En outre, la surveillance doit être menée de manière cohérente, ciblant les terroristes et autres personnes qui constituent une menace pour la sécurité nationale.

Le Partenariat national :

- Renforcer la coopération entre toutes les parties prenantes des secteurs public et privé, y compris les experts en cyber sécurité, les opérateurs de réseaux de télécommunication et les fournisseurs de services Internet et la société civile ;

- Sensibiliser les citoyens et les autorités aux menaces que le cyber univers représente pour la société ;

Une stratégie nationale :

- Une stratégie de gestion des risques utilisée pour identifier et caractériser les cybermenaces, savoir évaluer la vulnérabilité des actifs critiques à ces menaces, identifier les risques et se procéder rapidement à les réduire avant que la vulnérabilité ne se transforme en une attaque efficace.

[1] Mémoire « assurance des risques cybernétiques » ; Abbes Yosra ;2018 ; p27

Coopération internationale :

- Coordonner les actions et conclure des accords avec d'autres pays concernant les crimes liés au cyber terrorisme et promouvoir l'échange d'informations et des bonnes pratiques liées à la prévention et la lutte contre le Cyberterrorisme.

4 - LES MOYENS DE PRVENTIONS ET LES BONNES PRATIQUES

Dans ce contexte, face aux cyber-risques, les bonnes pratiques suivantes sont recommandées :

Connaissance des risques :

- Procéder à un bilan-risque annuel pour réévaluer toute exposition aux risques, et poursuivre les actions de sensibilisation auprès des dirigeants pour maintenir le cyber-risque au rang de leurs priorités.

Élimination des vulnérabilités connues :

- Assurer la mise à jour régulière des matériels et des logiciels de sécurité, car c'est à force de persévérance que le cybercriminel atteint son but.
- Maintenir l'efficacité des protections de base.

Télétravail et mobilité :

- Définir des règles strictes d'accès aux données. À mesure que les appareils personnels investissent la sphère professionnelle, il est primordial de protéger le réseau indépendamment du périphérique d'accès.

Sensibilisation et formation :

- Former les salariés aux politiques et procédures d'intervention en déployant un programme de sensibilisation complet : campagnes d'affichage, conseils par e-mails, consignes de sécurité pour les nouveaux collaborateurs et formations annuelles sur ordinateurs.

Gestion des incidents :

- Établir, exécuter et tester régulièrement les plans de réponse.

Monitoring :

- Surveiller en permanence tous les systèmes d'information et de communication, ainsi que les journaux associés, pour détecter et neutraliser d'éventuelles attaques.

Sécurisation du réseau :

- Gérer le périmètre du réseau et filtrez les accès non autorisés.

Protection anti-malware :

- Établisse des défenses anti-malware et effectuez en permanence des analyses de détection.

Établissement d'un règlement intérieur pour l'utilisation des réseaux sociaux :

- Les réseaux sociaux deviennent peu à peu l'un des principaux vecteurs du cybercrime, sensibilise les collaborateurs aux règles de base d'une utilisation professionnelle acceptable et à des comportements responsables hors du travail.

Diagnostic de sécurité :

- Au moment d'acquérir les produits ou services des fournisseurs, puis au moins une fois par an, vérifiez leur respect de vos politiques internes et des obligations légales et réglementaires en vigueur.

CONCLUSION

Le cyber risque est un risque qui préoccupe : assureurs, professionnels et particuliers y sont exposés. Avec un nombre d'attaque fortement croissant, le caractère migrant du type d'attaques et leur diversité en fait un risque difficile à appréhender. Aujourd'hui, force est de constater que le marché de l'assurance cyber des particuliers se développe, répondant à une demande croissante de protection des assurés. De nouvelles offres ne devraient pas tarder à voir le jour, s'adaptant ainsi de manière toujours plus ciblée au nouveau visage de ce risque.

Nous allons passer par la suite au deuxième chapitre en essayant d'analyser le questionnaire afin de dégager un aperçu général sur la conscience d'un échantillon cible (les banques) concernant la gravité des risques cybernétiques d'une part et sur leur acceptabilité vis-à-vis d'un nouveau produit assurantiel visant à couvrir ces risques d'autre part.

CHAPITRE II : LA CONCEPTION ET LA COMMERCIALISATION DU PRODUIT « ASSURANCE DES RISQUES CYBERNETIQUES »

CHAPITRE II : LA CONCEPTION ET LA COMMERCIALISATION DU PRODUIT « ASSURANCE DES RISQUES CYBERNETIQUES »

INTRODUCTION

Les contrats cyberassurance ont pour ambition de protéger les assurés contre les atteintes au système d'information et aux données qu'il contient et d'apporter une réponse adaptée à un risque complexe, le mécanisme contractuel permet aux assureurs de définir librement les risques et garanties ainsi que le fonctionnement du contrat dans la limite du respect de la loi. La prise en charge du risque cyber diffère donc indéniablement d'un assureur à l'autre par la définition des garanties accordées, les plafonds, les franchises, les sous-limites, et les exclusions.

SECTION 1 : ÉTUDE DE MARCHÉ

1 - LA STRUCTURE DU QUESTIONNAIRE :

Une enquête est une activité organisée et méthodique de collecte de données sur des caractéristiques d'intérêt d'une partie ou de la totalité des unités d'une population à l'aide de concepts, de méthodes et de procédures bien définis. Elle commence habituellement s'il y a un besoin d'information et s'il n'y a pas de données ou si elles sont insuffisantes.

Dans le cadre d'une étude du marché national, comme il est le cas pour tout nouveau produit, on a préparé une enquête, destinée particulièrement aux banques afin de dévoiler leur niveau de conscience concernant l'enjeu de la sécurité cybernétique et l'importance d'un produit assurantiel futur qui vise à protéger les entreprises en général des conséquences graves d'une attaque ou erreur cybernétique.

Le questionnaire comporte des questions réparties sur quatre sections, chaque section se focalise sur un axe particulier de l'étude comme suit :

- La section A : comporte quatre questions simples qui ont pour objectif de collecter quelques informations générales.
- La section B : contient sept questions destinées à évaluer la performance de système d'information de banques interviewées.
- La troisième partie du questionnaire, vise à évaluer le poids des incidents cybernétiques dans les banques à travers sept questions

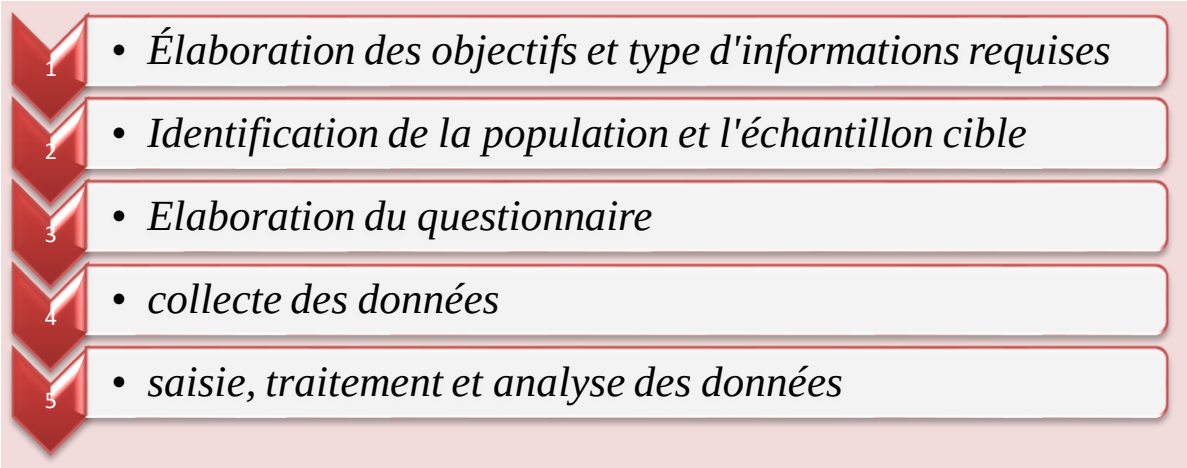
- Enfin, la quatrième section qui comporte trois questions, présentant spécifiquement le produit « assurance des risques cybernétiques » pour susciter l'intérêt des parties concernées pour ce produit.

Le questionnaire serait alors diffusé aux18banques algérienne, qui ont répondu à la majorité des questions malgré la confidentialité de l'information liée surtout à un sujet délicat. Ci-dessous la liste des banques contactées

LISTES DES BANQUES
Arab Banking Corporation Algeria (ABC)
Banque AL Baraka d'Algérie
Banque Africaine de Développement(BAD)
Banque de l'Agriculture et du Développement Rurale (BADR)
Banque de Développement Local (BDL)
Banque Extérieure d'Algérie (BEA)
Banque Nationale d'Algérie (BNA)
CITIBANK
Caisse Nationale d'Epargne et de Prévoyance-Banque (CNEP)
Crédit Populaire d'Algérie (CPA)
Gulf Bank Algérie (AGB)
AL SALAMA BANK Algeria
Arab Bank PLC ALGERIA
BNP PARIBAS EL-djazair
FRANSABANK AL-Djazair
NATIXIS ALGERIE
SOCIETE GENERALE Algérie
TRUST BANK Algérie

La démarche de l'enquête est résumée dans la figure suivante :

Figure n° (II.10) : Étapes de structure de questionnaire



2 - ANALYSE DU QUESTIONNAIRE :

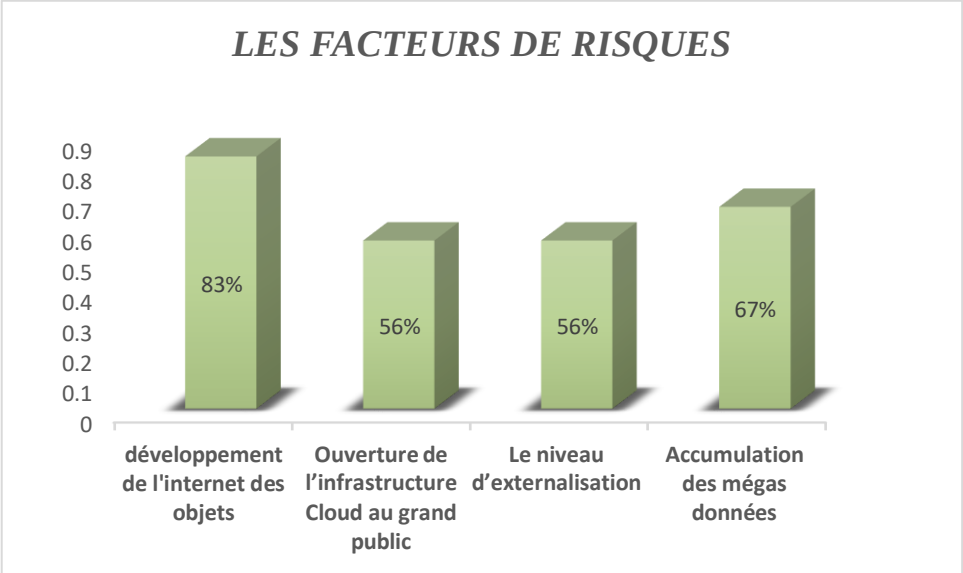
Nous avons sélectionné un échantillon de 18 banques algériennes, publiques et privées, et les avons contactées par e-mail ou par entretiens sur place, nous avons obtenu 18 questionnaires remplis en bonne et due forme, sur lesquels nous nous sommes basés pour faire l'analyse nécessaire.

Après avoir établi la base de données sur SPSS (Statistical Software Package for Social Sciences) et généré les données statistiques et graphiques nécessaires pour interpréter les résultats, nous analyserons les questions une par une selon l'ordre dans lequel elles apparaissent dans le questionnaire.

2.1 - Informations générales

a) Veuillez évaluer les facteurs qui entraînent un changement important du niveau de risque cybernétique au cours des dix dernières années

Figure n° (II.11) : classification des facteurs de risques par les banques



La réponse à la question posée réside dans l'évaluation de quatre facteurs de risque, qui ont une influence primordiale, moyenne ou faible sur l'évolution des risques cybers. Selon l'histogramme ci-dessus, dans le développement du risque cyber, 83% des réponses soutiennent le développement de l'internet des objets et l'importance d'accumuler 67% de données à

volumineuse échelle. Le niveau d'ouverture et d'externalisation de l'infrastructure cloud arrivent en dernier atteignant un taux de 56%

Le développement de l'internet des objets a ouvertement, un rapport énorme avec la propagation de ce risque puisqu'il est lié à nos habitudes quotidiennes. On utilise l'internet pour exécuter les tâches journalières les plus simples et par conséquent nos informations confidentielles existent partout et la question qui se pose est la suivante: Sommes-nous authentiquement prêts à ce développement exponentiel sur le plan sécurité informatique pour tronquer au minimum la probabilité de l'occurrence des incidents cybers ?

b) Considérez-vous que votre organisme est menacé par des cyber-attaques ?

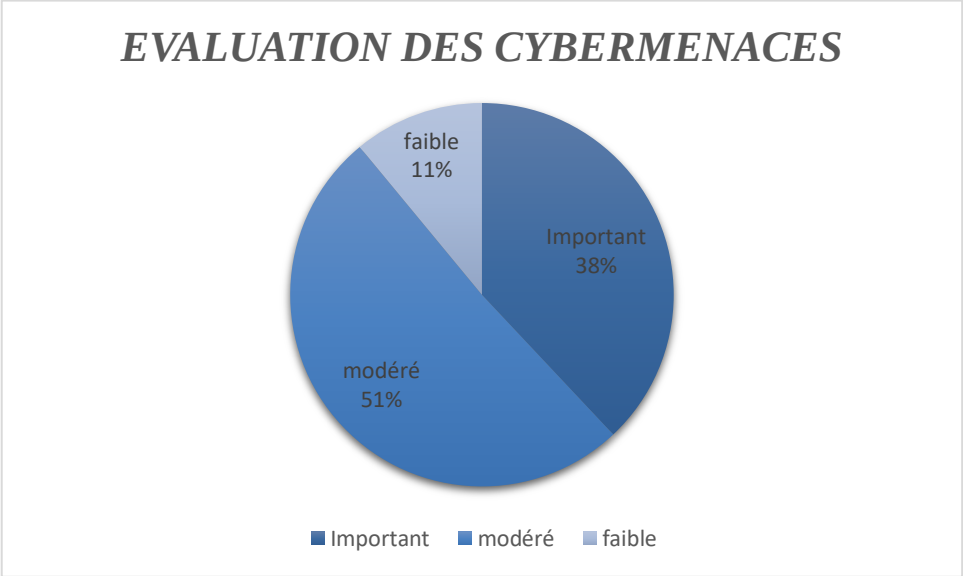
Tableau n° (II.02) : le pourcentage des cyberattaques

		Effectifs	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	OUI	18	100,0	100,0	100,0

Source : SPSS

Pour cette question, toutes les personnes interrogées étaient d'accord à 100%, SPSS a considéré cette variable comme constante puisqu'on a la même réponse pour tout l'échantillon. Nous avons demandé par la suite d'évaluer le niveau de risque perçu ;

Figure n° (II.12) : Évaluation des cybermenaces

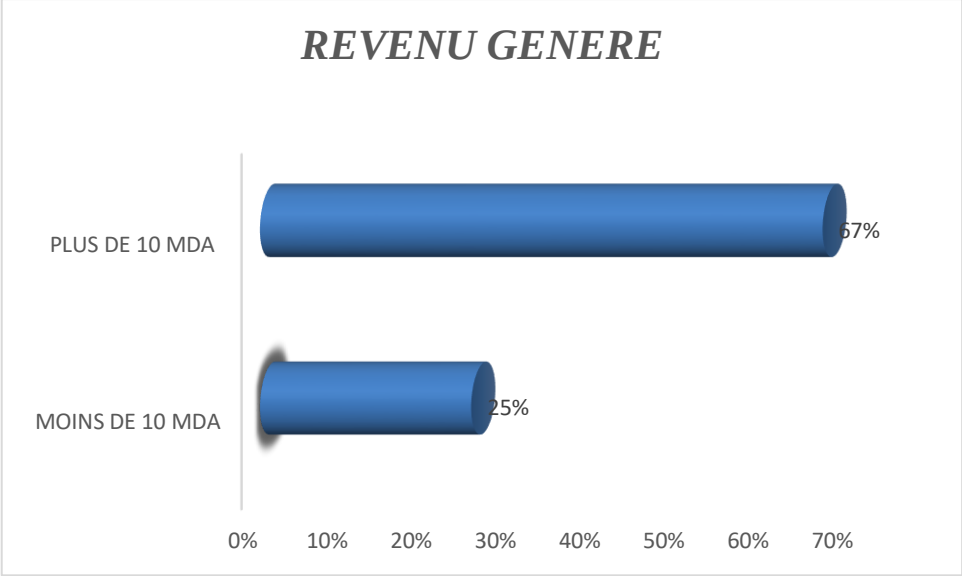


Le camembert montre que 38% des répondants estiment que les cybermenaces sont très cruciales, 51% la considère comme modérée alors que 11% affirment qu'elle est encore faible. Cette question avait pour objectif de tester la conscience des sociétés bancaires concernant l'existence, d'abord, d'une menace cyber et surtout de degré de sévérité de cette menace.

c) Avez-vous un site web de commerce ou de service en ligne ?

55,6% de l'échantillon ont confirmé ne pas avoir de site Web de commerce ou de service en ligne, tandis que le reste de l'échantillon a estimé la part des revenus générés par le site Web, comme le montre la figure ci-dessous.

Figure n°(II.13) : Estimation du revenu généré des sites web



Le e-commerce apparait comme une cible choix pour les cybercriminels, les site web de commerce ou de service en ligne sont effectivement très convoités par les pirates informatiques en raison de leur présence croissante sur le marché et de la richesse des informations détenues (noms des clients, coordonées bancaire…), les entreprises bancaires dotées de sites Web commerciaux sont plus susceptibles d'être exposées aux cybermenaces.

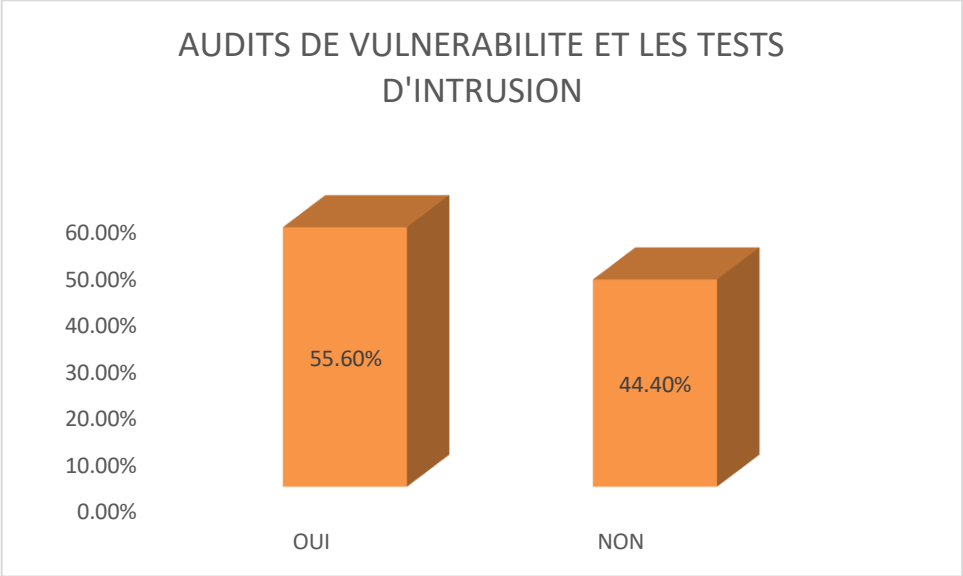
2.2 - Sécurité des systèmes d'information :

À travers cette partie, nous continuons à étudier les composants de sécurité informatique de la banque afin de juger sa performance.

a) Effectuez-vous régulièrement des audits de vulnérabilité et/ou des tests d'intrusion ?

Les audits de vulnérabilité et les tests d'intrusion consistent à tester le système d'information afin de déceler toute vulnérabilité possible. Ils servent à évaluer le risque de piratage et d'identifier des pistes pour en réduire sa portée.

Figure n° (II.14) : Les audits de vulnérabilités et les tests d'intrusions

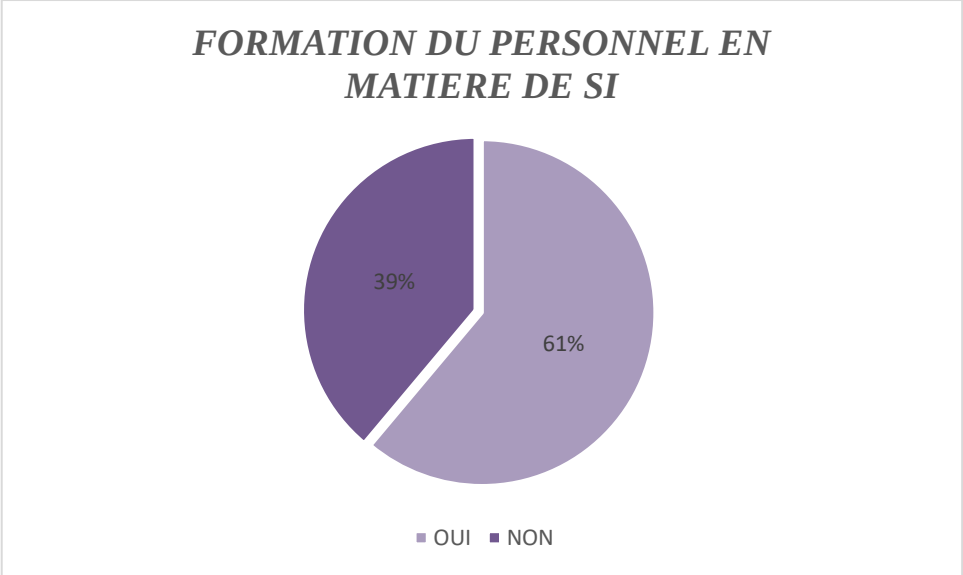


Le graphique ci-dessus montre que 55,6% des banques interrogées ont confirmé que le système de sécurité informatique de leur entreprise fonctionnait bien grâce aux tests quotidiens et 44,4% des entreprises ont déclaré qu'elles n'avaient effectué aucun test de vulnérabilité ou d'intrusion. Ce qui signifie la performance de leur système demeure faible. Ce jugement dépend plus ou moins de la recommandation de la personne interrogée.

b) Est-ce que l'ensemble du personnel reçoit une formation ou une sensibilisation aux risques cyber et aux bonnes pratiques de l'hygiène de sécurité informatique ?

61% des interviewés ont confirmé que les employés ont reçu une formation régulière en matière de sécurité informatique tandis que 39%ne sont pas sensibilisés à la gravité de la menace cyber et ils n'ont aucune maitrise sur les moyens de sécurité qui leur permettront de préserver les données confidentielles. L'absence ou le manque de formation de personnel dans ce domaine, peut entrainer un risque opérationnel.

Figure n° (II.15) : le pourcentage du personnel formé en SI au sein de la banque



La relation entre la performance du système de sécurité informatique et la formation du personnel est forte et le test du Khi-deux de SPSS s'est avéré significatif (niveau de signification de **0,025 <0,05**). Nous choisissons le test du Khi-deux parce que nous voulons tester l'influence d'une variable qualitative sur une autre. Nous avons obtenu les résultats suivants :

Tableau n°(II.03): test de Khi-deux entre la performance de système SI et la formation du personnel

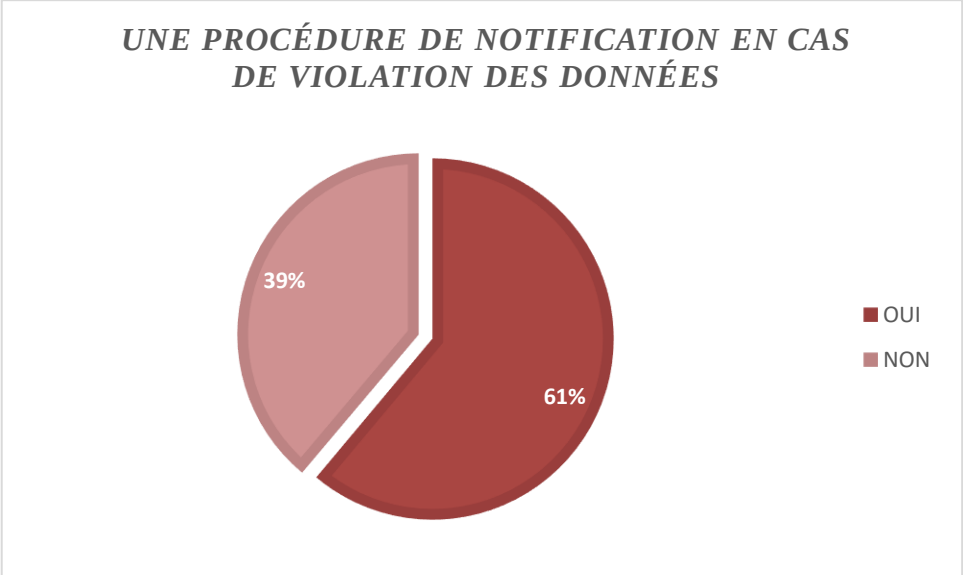
	Valeur	ddl	Signification asymptotique (bilatérale)	Sig. exacte (bilatérale)	Sig. exacte (unilatérale)
khi-deux de Pearson	5,000[a]	1	,025		
Correction pour continuité[b]	2,813	1	,094		
Rapport de vraisemblance	5,178	1	,023		
Test exact de Fisher				,089	,047
Association linéaire par linéaire	4,667	1	,031		
N d'observations valides	18				

c) Avez-vous mis en place une procédure de notification aux individus et au régulateur en cas de violation des données ?

Une violation des données risque d'entrainer une série d'effets négatifs importants pour l'établissement concerné et il doit veiller à atténuer l'effet de toute violation en établissant une procédure de notifications qui visent à assurer une plus grande sécurité des données.

Par conséquent, cette question était posée pour s'assurer que les banques suivent les mesures de sécurité les plus élémentaires.

Figure n° (II.16) : procédure de notification en cas de violation de données

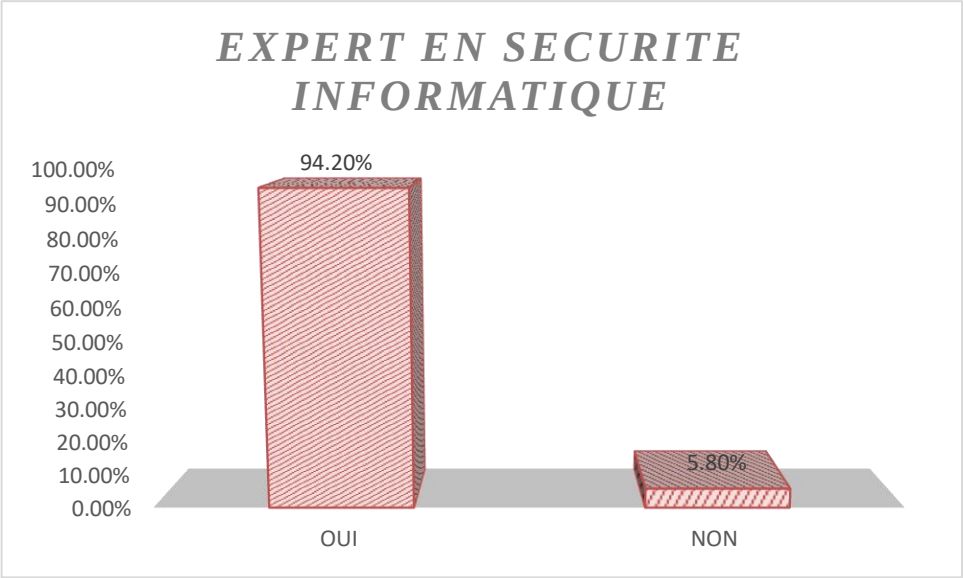


Dans ce cas, 61% des répondants ont confirmé qu'ils se sont conformés à ces mesures, tandis que39% confirment le contraire. Le fait que (1/3) des banques n'aient pas mis en œuvre la procédure de notification en cas de violation de données constitue une menace pour la sécurité de leur système informatique qui devient propice à la survenance de failles

d) Votre entreprise dispose t'elle d'au moins d'un expert en sécurité informatique et protection des données ?

Les experts en sécurité informatique sont tenus de diagnostiquer le système d'information de la banque afin de déceler toute faiblesse et d'assurer sa pérennité. Presque toutes les personnes interrogées ont confirmé que leur organisation dispose d'experts. Elles représentent 94,2% de l'échantillon et les 5,8% restants n'ont pas d'experts. Cela peut causer de graves problèmes, il est donc très susceptible d'être soumis à des cyberattaques.

Figure n° (II.17) : Avoir un expert en sécurité informatique



2.3 - Risques cybernétiques :

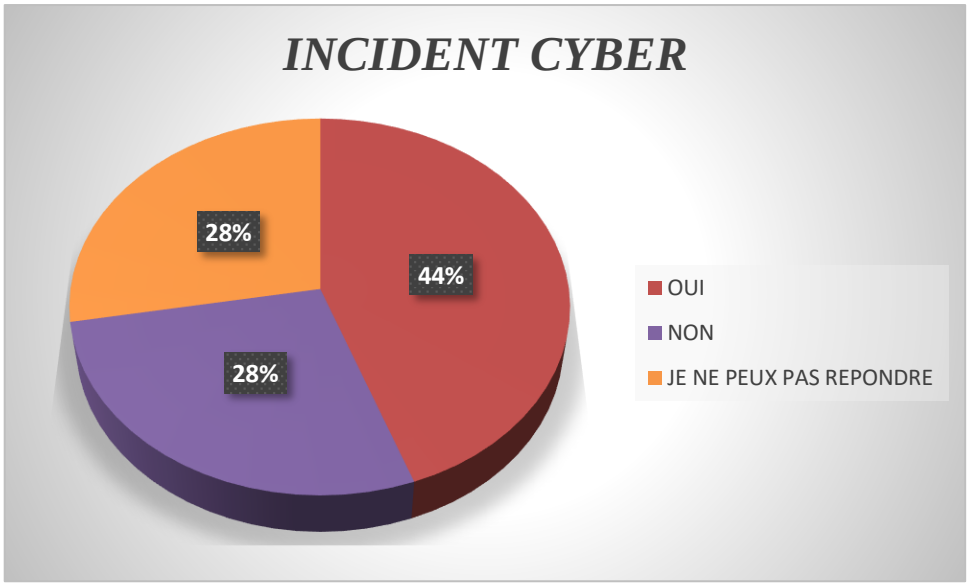
Par le biais de cette partie nous continuerons d'explorer le volet risques cybernétiques afin de souligner le poids de ces derniers sur l'activité bancaire

a) Avez-vous été victime d'une attaque Cyber ?

Du point de vue de la confidentialité, c'est la question la plus critique et pour favoriser les chances d'obtenir des réponses proches de la réalité, une troisième option « Je ne peux pas répondre » a été ajoutée, ce qui crée une certaine nuance, qui est une affirmation déguisée.
De plus, comme le montre la figure ci-dessous, 28% des répondants ont opté pour cette option, alors que 44% des répondants ont confirmé avoir été victimes d'un incident cyber et 28% ont déclaré n'avoir jamais subi de telles attaques.

En quelque sorte, nous pouvons tirer la conclusion que, intentionnellement ou non, plus des deux tiers des échantillons étudiés ont été endommagés par des cyberattaques.

Figure n° (II.18) : Victime d'un incident cyber

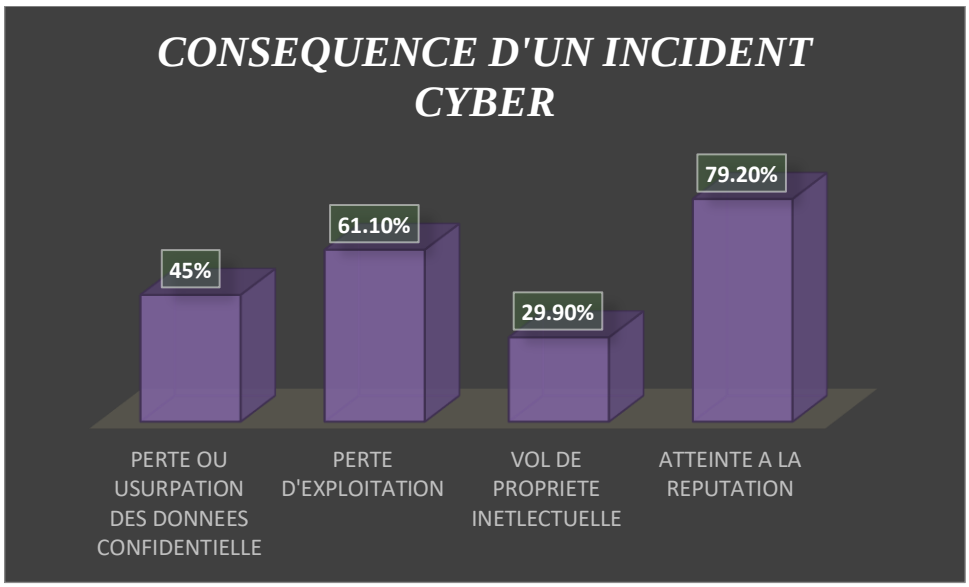


i. Si oui, quelles ont été les conséquences de cette attaque/erreur ?

Cette question est adressée à ceux qui ont confirmé avoir été victime d'un incident cybernétique, nous avons présenté ici, quatre types de pertes comme suit :

- Perte ou usurpation de données confidentielles
- Pertes d'exploitation
- Vol de propriété intellectuelle
- Atteinte à la réputation

Figure n° (II.19) : Les conséquences d'une attaque cyber

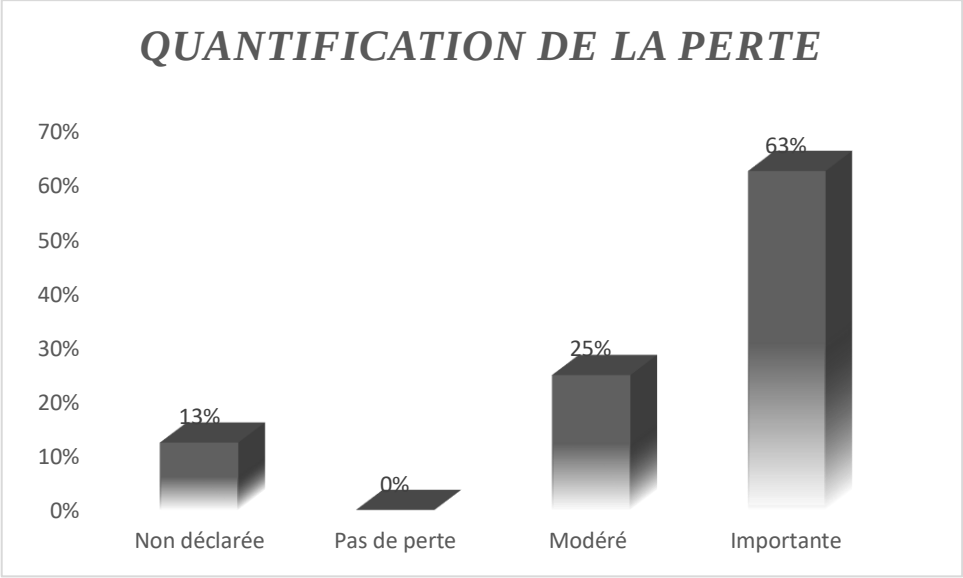


Pour cette question, les répondants avaient la possibilité de sélectionner plus d'une option la quasi-totalité des interviewés victimes d'un incident cyber ont subi une perte de l'atteinte à la réputation avec un pourcentage de 79.2%, 61.1%, ont subi des pertes d'exploitation, 45% ont subis des pertes ou usurpation de données confidentielles et 31.2% ont subis des pertes de vol de propriété intellectuelle.

ii. Si oui, comment /combien quantifiez-vous la perte ?

Cette question vise à déterminer la perte des interviewés qui ont été affectés par un cyber incident.

Figure n° (II.20) : La quantification de la perte cyber



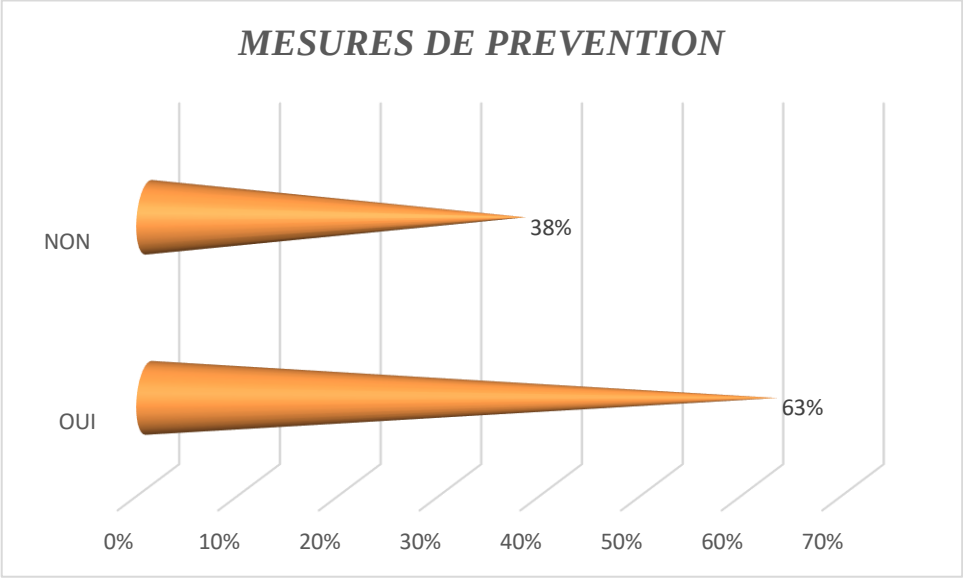
On constate que 25% des victimes ont qualifié la perte comme « Modérée », tandis que 63% l'ont considérée comme « Importante » ce qui représente plus de la moitié de l'échantillon, chose qui est solennelle à mon avis. Personne n'a affirmé qu'il n'y avait pas de perte alors que 13% ont considéré qu'il y avait une perte non déclarée (personne n'a fourni des chiffres exacts)

b) Des mesures ont-elles été prises pour éviter le renouvellement des sinistres de même nature que ceux déjà survenus ?

62% des banques ont répondu qu'elles avaient pris des mesures pour éviter tout renouvellement des sinistres liés aux cyberattaques, ce qui est une bonne chose car cela permet de réduire la possibilité de venir victime de cyber risques et de prévenir par la suite

d'éventuelles cyberattaques bien que 38% des personnes interrogées aient déclaré ne pas avoir pris les mesures nécessaires après la cyberattaque, cette question montre le niveau de sensibilisation de chaque banque.

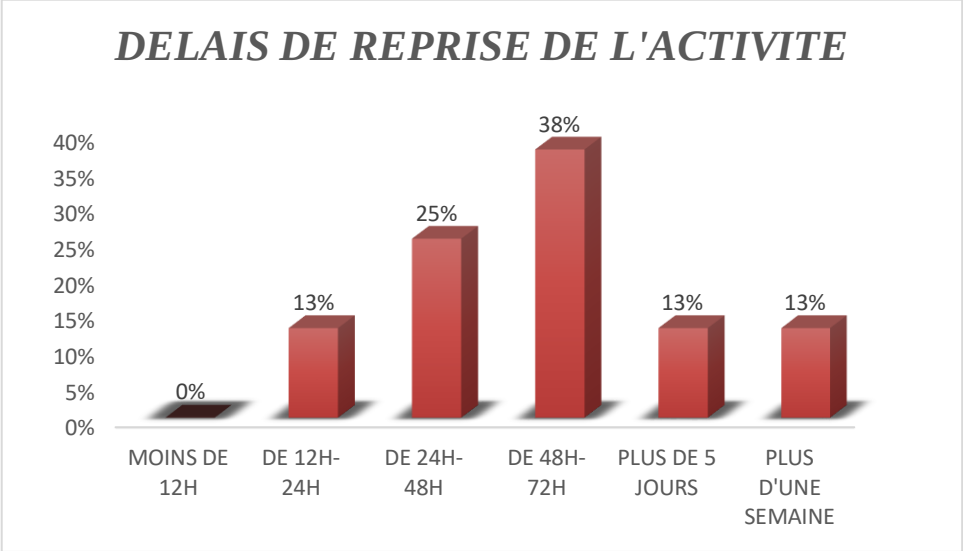
Figure n° (II.21) : Les mesures de prévention



c) Le délai nécessaire à la reprise d'activité en cas d'incident sur vos systèmes d'information est-il estimé à plus de 12h ? (Si oui combien du temps ?)

À partir du délai nécessaire de la reprise de l'activité, la banque mettra en place un plan de continuité d'activité, cette procédure aura pour objectif d'assurer une disponibilité en continu des activités les plus vitales de la banque

Figure n° (II.22) : Le délai nécessaire à la reprise de l'activité bancaire



Nous avons demandé aux personnes interrogées d'estimer le temps nécessaire à la reprise de l'activité bancaire ; 13% des répondants ont dit qu'il leur faudrait plus d'une semaine pour se rétablir, avec le même pourcentage les interviewés ont indiqué qu'ils auraient besoins plus de 5 jours, bien que 38% ont pris de 48h à 72 h. plus le délais de la reprise est long plus les pertes d'exploitation de la banque sont importantes.

2.4 - L'assurance des risques cybernétiques :

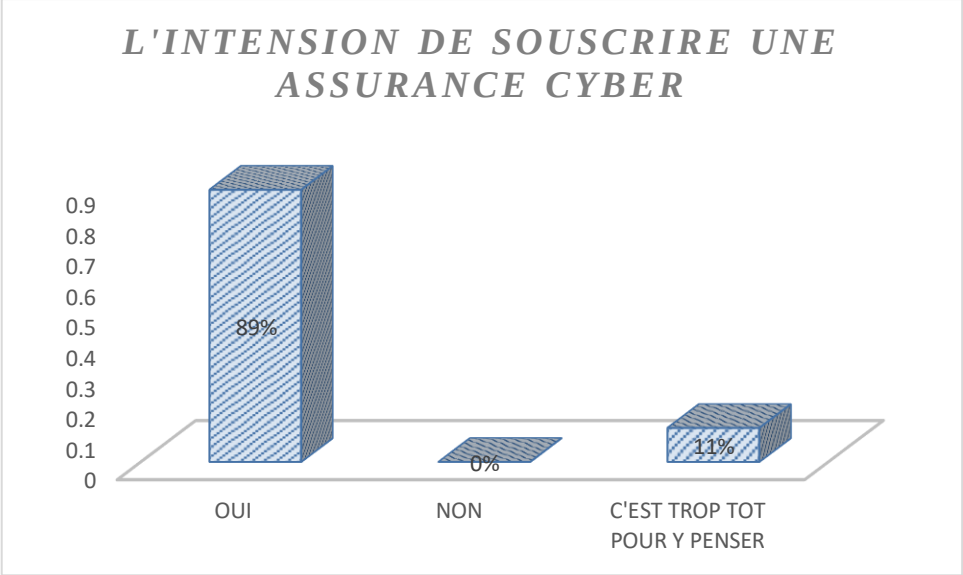
a) Avec la révolution numérique et digitale en Algérie, prévoyez-vous de souscrire une assurance cybernétique pour faire face aux coûts inhérents à une erreur ou une attaque cyber ?

C'est est la question clé du questionnaire, à laquelle peuvent répondre les trois options suivantes ;

- Oui
- non
- Il est trop tôt pour y penser ;

Nous avons obtenu les résultats suivants :

Figure n° (II.23) : L'intention de souscrire une assurance cybernétique



Seuls 11% des sondés estiment qu'il s'agit d'une sorte d'assurance pour l'avenir, est ce que c'est trop tôt pour y envisager, mais ils croient aussi en l'importance de ce produit avec la révolution numérique et technologique. La plupart (89%) ont manifesté un grand intérêt pour ce nouveau produit d'assurance. Aucune des personnes interrogées n'a déclaré ne pas avoir l'intention de souscrire une assurance cybernétique à l'avenir.

Selon la recherche menée, il n'y a pas de lien direct entre le fait d'avoir été victime d'un incident cyber et l'intention ou la décision de souscrire une cyberassurance, ce qui peut clairement refléter le haut niveau de compréhension de la cyberassurance par les interviewés, Se soucier de la nécessité de prévenir d'éventuelles pertes même si elles n'ont jamais subi de telles pertes auparavant, ce qui se fait dans le cadre du principe *« **mieux vaut prévenir que guérir ».***

Nous avons testé l'indépendance entre le fait d'avoir été victime d'un incident cyber et la volonté de souscrire une assurance cyber, et le test Khi-deux donne les résultats suivants

Tableau n° (II.04) : test de dépendance entre le fait d'avoir été victime d'un incident cyber et l'intention de souscrire une assurance cyber

	Valeur	ddl	Signification asymptotique (bilatérale)
khi-deux de Pearson	1,576[a]	4	,813
Rapport de vraisemblance	1,925	4	,750
Association linéaire par linéaire	,162	1	,687
N d'observations valides	18		

L'analyse d'indépendance utilisant le test du Khi-deux montre que la décision de souscrire une assurance cybernétique n'est pas affectée par le fait d'être une victime d'un cyber-incident, ce qui prouve la conscience des banques envers l'importance de se prémunir des conséquences du risque cybernétique en souscrivant une police cyber.

Cette affirmation s'appuie sur la valeur du test khi deux qui est égale à : 1,576, le degré de liberté de 4 et la signification asymptotique bilatérale qui est dans ce cas : **p= 0,813 > 0,05** (non significatif).

b) Si oui, quelles sont les couvertures que vous jugez utiles ?

L'interviewé est invité à sélectionner une série de couvertures directes et indirectes ; puis à les classer en fonction de leur sévérité : forte, moyenne ou faible

i. *Couvertures directes* [1]

- ***Gestion de crise***

La gestion de crise couvre les heures et les jours de pertes qui suivent un incident cybernétique tant en gestion interne de la situation qu'en terme de communication externe.

Elle couvre principalement les couts pour des services spécifiques afin de rétablir la réputation de la société ainsi que les coûts de transmission de l'information aux actionnaires et aux clients

[1]Institut canadien des actuaires, Casualty Actuarial Society et Society of Actuaries.2017.

- ***Perte d'exploitation***

La compagnie d'assurance garantira à l'assuré les pertes d'exploitation subies à la suite d'une interruption d'activité due à l'inaccessibilité totale ou partielle du système informatique des société assurées dès lors qu'elle est causée par un évènement perte d'exploitation , elle sert à couvrir les sommes perdues du fait de l'impossibilité de travailler c'est à-dire la part des charges fixes et du résultat d'exploitation qui correspond à la partie non réalisée du chiffre d'affaires suite à un incident cybernétique.

- ***Protection de la base de données***

Elle couvre les frais de la reconstitution de la base de données de la société.

- ***Fraude***

Cette couverture est destinée à couvrir les conséquences d'une fraude qu'elle soit interne ou externe.

- La fraude externe : des actes malveillants d'escrocs visant à extorquer indirectement de l'argent aux sociétés en leur faisant via des subterfuges très sophistiqués visant à se faire remettre frauduleusement des fonds ou des marchandises ;
- La fraude interne : les actes malveillants du personnel : vol de données, divulgation d'informations sensibles.

- ***La propriété intellectuelle***

Elle couvre les pertes suite à un vol ou une divulgation des créations intellectuelles (Les nouvelles idées de projets, d'applications, les stratégies innovatrices…) .

- ***Cybercriminalité***

C'est une couverture pour les coûts d'investigation et les indemnités des pertes du piratage. Elle couvre aussi les rançons demandées par les hackers pour restaurer des bases de données ou sites internet qu'ils ont bloqués.

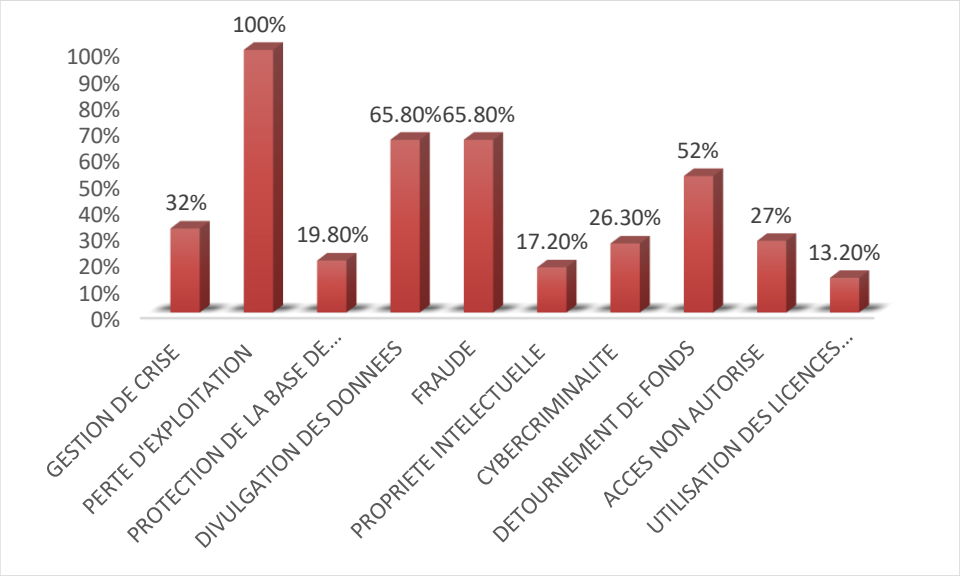
- ***Détournement de fonds***

Elle couvre les frais d'expertise et l'assistance informatique, les frais de protection juridique ainsi que les pertes pécuniaires suite à une escroquerie, un abus de confiance ou usage de faux.

- ***Utilisation des licences piratées***

Elle couvre les couts de réparation et récupération de toute information et données perdues suite à l'utilisation des logiciels piratés. Pour le choix des couvertures directes, les pourcentages suivants ont été obtenus

Figure n° (II.24) : Sélection des couvertures directes



La réponse pour cette question est multiple, chaque interviewé peut choisir une ou plusieurs garanties, nous constatons que la couverture la plus demandée est celle qui couvre la perte d'exploitation avec un pourcentage de 100%, suivie, des couvertures contre la fraude et le détournement de fonds à pourcentages égaux de 65.8%. La couverture la moins demandée par les interviewés est la protection de la propriété intellectuelle avec un pourcentage de 13.2%.

Par conséquent, nous pouvons conclure qu'en termes de cyber-risque, les pertes d'exploitation et la fraude sont les principales considérations de la banque, tandis que la propriété intellectuelle constitue le dernier souci.

ii. *Couvertures indirectes* :

Dans cette question, on a proposé un éventail de trois types de responsabilités civiles :

- ***La responsabilité civile liée à l'utilisation frauduleuse de données de la clientèle.***

Elle couvre principalement :

La surveillance de la fraude ou autres services connexes aux clients touchés par un cyber-événement :

- La responsabilité civile, frais de défense et de réclamation, amendes et frais de défense réglementaires ;
- La responsabilité indirecte lorsque le contrôle de l'information est externalisé,
- Le contrôle de crise par exemple, coût de notification des parties prenantes, enquêtes, frais légaux ;
- La surveillance de la fraude ou autres services connexes aux clients touchés par un cyber-événement ;
- La protection contre le vol d'identité pour les clients.

➢ ***Responsabilité civile atteinte à la sécurité de réseau***

Toute utilisation divulgation ou transmission non autorisée par l'assuré de données personnelles ou informations confidentielles et compris toute transmission de virus / logiciel malveillant à un tiers

Elle couvre les coûts résultants de la réintégration des données (restaurer ou recréer des données et des logiciels pour des tiers) ainsi que le coût résultant d'une procédure judiciaire suite à l'insertion d'un virus informatique causant des dommages à un tiers, un accès non autorisé de l'assuré causant des dommages à un système d'une tierce partie, une perturbation de l'accès autorisé par les clients ou bien un détournement de la propriété intellectuelle.

➢ ***Responsabilité civile visant la communication et les médias***

Elle couvre les frais de défense et de réclamation (amendes), les frais de défense réglementaires suite à une violation du software. Les interviewés ont choisi les couvertures indirectes qu'ils souhaitent.

Figure n° (II.25) : Sélection des couvertures indirectes

Leur premier choix était la responsabilité civile sécurité du réseau avec 71% des avis. En effet, chaque entreprise est tenue de se prémunir à l'aide d'une protection des informations privées vu que plusieurs informations à caractère confidentiel existent dans leurs serveurs tels que les coordonnées, les renseignements médicaux et les dossiers relatifs aux clients. Il est primordial donc qu'ils disposent d'une garantie qui sert à couvrir leur responsabilité à l'égard de ces informations en cas d'une intrusion externe ou bien interne de leurs systèmes informatiques.

iii. Les besoins exprimés par les prospects en termes des couvertures

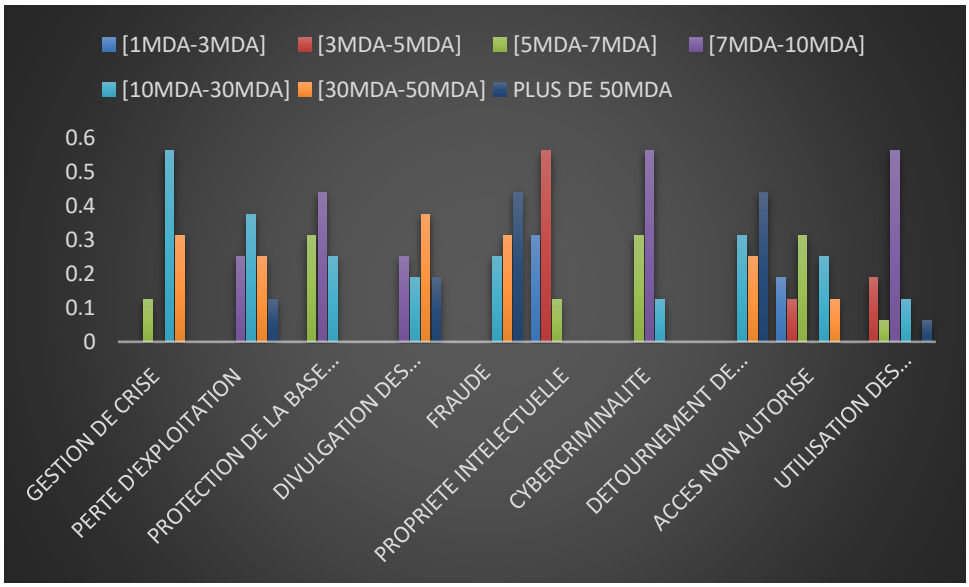
Nous avons demandé aux banques interviewées d'estimer le montant limite de la garantie requises (directe et indirectes), Le coût annuel d'une assurance cyber-risque dépend de la taille de l'entreprise et du plafond de garantie souhaité. Chaque banque a proposé une limite de couverture, le montant du contrat sera calculé par la suite selon :

1. Son secteur d'activité et niveau de sensibilité des données qu'elle exploite, ainsi que son volume ;
2. Le chiffre d'affaires que réalisé, (plus il est important, plus la prime la sera aussi) ;
3. Le nombre et le type de garanties qu'elle souhaite contracter, (plus elles sont nombreuses, plus le prix de son assurance sera élevé, notez que certaines d'entre elles valent (très) cher, comme par exemple la garantie rançon en cas d'extorsion de vos données) ;

4. La performance de son système d'information, c'est-à-dire le fait que ces données soient déjà sécurisées, ou non (le montant des cotisations sera moins important si vos employés effectuent des sauvegardes régulières des données, par exemple).

La figure ci-dessous montre les montants limités des garanties fournies par les banques concernées.

Figure n° (II.26) : Limites des garanties directes



La majorité des interviewés ont proposé une fourchette allant de 10MDA à 30MDA pour la garantie gestion de crise avec un pourcentage de 56.3%, un pourcentage de 37.5% été proposé pour la garantie perte d'exploitation, les garanties cybercriminalité, utilisation des licences piratés, et protection de la base de données Les garanties contre la cybercriminalité, l'utilisation de licences piratées et la protection des bases de données ont été combinées dans une fourchette de [7MDA à 10MDA], et la limite des garanties de fraude et de détournement est estimé à plus de 50MDA.

Afin de déterminer le prix d'une assurance cyber, nous regroupons le montant fourni par chaque banque en plusieurs fourchettes, de sorte que chaque fourchette soit associée à un taux qui dépend de la valeur du plafond des garanties ; Le tableau ci-après montre les fourchettes proposées pour chaque garantie :

Tableau n° (II.05) : le pourcentage des limites de couvertures par chaque garantie

Couvertures directes/lim	[1MDA-3MDA]	[3MDA-5MDA]	[5MDA-7MDA]	[7MDA-10MDA]	[10MDA-30MDA]	[30MDA-50MDA]	PLUS DE 50MDA
Gestion de crise			12,50%		56,30%	31,30%	
Perte d'exploitation				25%	37,5	25%	12,50%
Protection de la base de données			31,30%	43,80%	25%		
Divulgation des données				25,00%	18,80%	37,50%	18,80%
Fraude					25%	31,30%	43,80%
Propriété intellectuelle	31,30%	56,30%	12,50%				
Cybercriminalité			31,30%	56,30%	31,30%		
Détournement de fonds					31,30%	25%	43,80%
Accès non autorise	18,80%	12,50%	31,30%		25%	12,50%	
Utilisation des licences pirates		18,80%	6,30%	56,30%	12,50%		6,30%

« Le prix[1] de l'assurance cyber-risque se situe généralement entre **0,5%** et **5%** du **montant maximum assuré**, c'est aux réassureurs et assureurs de déterminer le taux à appliquer pour un ou la mutualité des assurés »

SECTION 2 : CONCEPTION DU PRODUIT

1 - UN CONTRAT D'ASSURANCE DES RISQUES CYBERNETIQUES

GÉNÉRALITÉ :

Les conséquences du cyber-risque pour sa victime étant complexes et variées, les compagnies d'assurance sont amenées à développer une panoplie de garanties à la hauteur des enjeux. En d'autres termes, les garanties proposées par les assureurs doivent être en mesure de considérer tous les aspects et conséquences de la survenance d'un cyber-risque.

En outre, l'assurance n'a pas pour but d'empêcher la réalisation d'un cyber-risque, il appartient donc à chaque entité qui subit un risque dans le cadre de son activité de mettre en œuvre toutes les mesures nécessaires à la protection de ses intérêts. À cette fin, la mise en place d'une cartographie des risques s'avère primordiale

Nombreuses sont les entreprises qui choisissent de souscrire à une assurance cybersécurité, du fait qu'elle représente la solution la plus sûre et la moins chère. En effet, avec

[1] https://www.aigassurance.fr/cyberedge.SUISSERE

cette solution, l'entreprise choisit de transférer le risque à défaut d'investir dans des solutions plus onéreuses sans toutefois garantir le risque zéro.

En revanche, les assureurs sont obligés d'imposer des critères minimums de sélection des risques, permettant d'éviter l'imprudence des entreprises à l'égard de ces risques très sensibles aux erreurs et défaillances humaines, ce qui se traduit par deux conséquences, d'une part, les assureurs améliorent la perception du cyber-risque dans les entreprises et leur permettent, d'autre part, de prendre conscience et de donner un caractère moral au risque évitant ainsi que le risque soit subjectif.

Une double raison explique le consentement des assureurs à offrir une garantie contre le cyber-risque :

- **Premièrement** : Pour de nombreuses compagnies d'assurance, l'assurance responsabilité civile est une branche très importante et rentable.
- **Deuxièmement** : le cyber-risque est une branche d'assurance qui gagne en importance et qui ouvre de nouvelles possibilités de revenus. De nombreux cyber-risques ne sont pas nouveaux, comme le vol de propriété intellectuelle, la perte de profits, la violation de la confidentialité et l'atteinte à la réputation. Mais cela n'empêche pas les compagnies d'assurance de créer de nouveaux produits et besoins en cyber sécurité.

2 - TYPES DE COUVERTURES

Il n'existe pas de contrat standard d'assurance cyber risques pour une entreprise. En effet, chaque compagnie définit librement les garanties que son offre contient. Cependant, l'on retrouve généralement 3 volets de protection, qui peuvent, selon les contrats, jouer en cas de :

- Dommages subis par votre société à la suite d'une attaque ou à une fraude informatique : virus, intrusion ou logiciel malveillant (ransomware, par exemple), violation de données personnelles et confidentielles…

a) Volet 1 : Les garanties d'assistance à la gestion de crise

Un piratage informatique provoque une crise dramatique au sein d'une entreprise. Il faut réagir vite et efficacement afin d'éviter la propagation de l'attaque et de limiter l'impact de

l'atteinte à l'image de votre entreprise. Les garanties d'assistance technique sont donc primordiales pour remettre en service votre système informatique et gérer la crise, en interne comme en externe. Voici les actions que mènera votre cyber assurance, qui s'appuie sur un réseau de professionnels spécialisés qu'elle peut mandater à tout moment :

- Mise à disposition d'experts en informatique pour rechercher la cause, réparer votre réseau informatique, reconstituer les données perdues, ainsi que pour sécuriser votre service ;
- Mise à disposition d'experts en communication et en relations publiques pour préserver l'e-réputation de votre entreprise (afin de maintenir la confiance de vos clients ou de vos investisseurs) et notifier le sinistre en cas de perte de données ;
- Mise à disposition d'experts juridiques en cas de mise en cause par des tiers (conseillers ou avocats spécialistes en cybercriminalité).

b) Volet 2 : Les garanties cyber dommages ou dommages aux biens

Ces garanties ont pour but d'assurer la pérennité de l'activité de la société en assumant l'impact pécuniaire que l'attaque informatique a pu coûter à l'entreprise. En effet, les conséquences financières peuvent être faramineuses ! Concrètement, à hauteur du plafond de garantie défini dans votre contrat, votre assurance prendra en charge :

- Les honoraires des experts dépêchés (informatique, communication ou juristes, par exemple) ;
- Les pertes d'exploitation liées à l'interruption de service suite à l'attaque ou à une perte de données ;
- Les surcoûts de fonctionnement et les frais nécessaires au redémarrage de votre activité (installation de nouveaux logiciels, notifications, enquêtes …) ;
- Le coût du remplacement des logiciels touchés par la malveillance informatique ;
- Les frais de négociation en cas de cyber extorsion, et dans le cas de rares contrats, le paiement de la rançon.

c) Volet 3 : Les garanties cyber responsabilité ou Responsabilité Civile

Suite à un piratage informatique, la responsabilité de votre entreprise peut être mise en cause par les autorités administratives et / ou par des tiers victimes d'un vol de leurs données, par exemple (souvent vos clients, mais aussi vos fournisseurs ou encore vos salariés). Contracter ces garanties vous permettra de voir les conséquences financières dues à ces réclamations prises en charge, à hauteur du plafond de garantie défini dans votre police :

- Les frais de défense juridique ;
- Le montant des dommages et intérêts réclamés par les tiers ayant subi un préjudice d'atteinte au respect de leur vie privée (altération ou diffusion de données personnelles et confidentielles) ou en cas de transmission de virus, par exemple ;
- Les amendes et / ou sanctions financières réclamées par les autorités (en cas de perte de données pas suffisamment protégées ou du manquement à l'obligation de notification).

Nous vous rappelons que chaque contrat est différent. Une cyber assurance peut ne vous proposer qu'une partie de ces garanties, comme vous pouvez choisir de n'en contracter que quelques-unes, selon les besoins de votre entreprise et les risques informatiques qu'elle encourt.

3 - LES EXCLUSIONS

Comme pour toutes polices d'assurances, les assurances cyber s'accompagnent de leur lot d'exclusions, c'est à dire des situations qui ne seront jamais prises en charge par votre assurance.

Il est courant qu'un contrat cyber risques n'assure pas les dommages matériels : elle ne prendra en charge que les dommages immatériels. Il faudra donc contracter une assurance tous risques informatiques ou encore un contrat dommages matériel informatique en complément de votre cyber assurance.

De plus, la plupart des cyber polices excluent d'office les pertes de données dues à une erreur humaine (de la part d'un salarié par exemple), comme la suppression involontaire des données conservées ou traitées par l'entreprise, ou encore le transfert par inadvertance de ces dernières à un tiers …

Dans la même idée, certains contrats excluent les dommages financiers liés à une fraude informatique en interne, ou encore ceux dus à une erreur de programmation.

Voici des exemples classiques d'exclusions que vous pouvez trouver dans un contrat de cyber assurance d'entreprise standard :

- Le montant des dommages matériels rendus inutilisable par l'attaque (ordinateurs, câbles…) ;
- Le prix des enquêtes (pour déterminer l'origine de l'attaque ainsi que l'identité du cyber criminel, dans le but de l'incriminer) ;
- Les sinistres résultant de l'utilisation de logiciel acquis illégalement, sauf si son utilisation l'est à votre insu ;
- Les frais d'amélioration de votre système informatique, des programmes et des données ou de votre système de protection contre les intrusions malveillantes ;
- Le coût des amendes, des pénalités et des sanctions administratives (en cas de vol de données) ;
- Les sinistres rendus possibles par l'absence d'un système de protection antivirus et firewall mis à jour régulièrement et activé en permanence, ou par une défaillance dans la protection du système d'information non remédiées dès la prise de connaissance.

Selon la compagnie d'assurance, sachez qu'une exclusion peut, en principe, être rachetée. Autrement dit, elle peut être levée si vous acceptez de payer une surprime (donc des cotisations plus importantes).

Avant de souscrire à un quelconque contrat, nous vous conseillons de faire appel à un expert (une société, un courtier ou un assureur spécialisé en cyber risques) qui effectuera ou fera réaliser une analyse de vulnérabilité, ou un audit des risques que court votre entreprise. Vous saurez ainsi quelles sont les garanties nécessaires à votre activité.

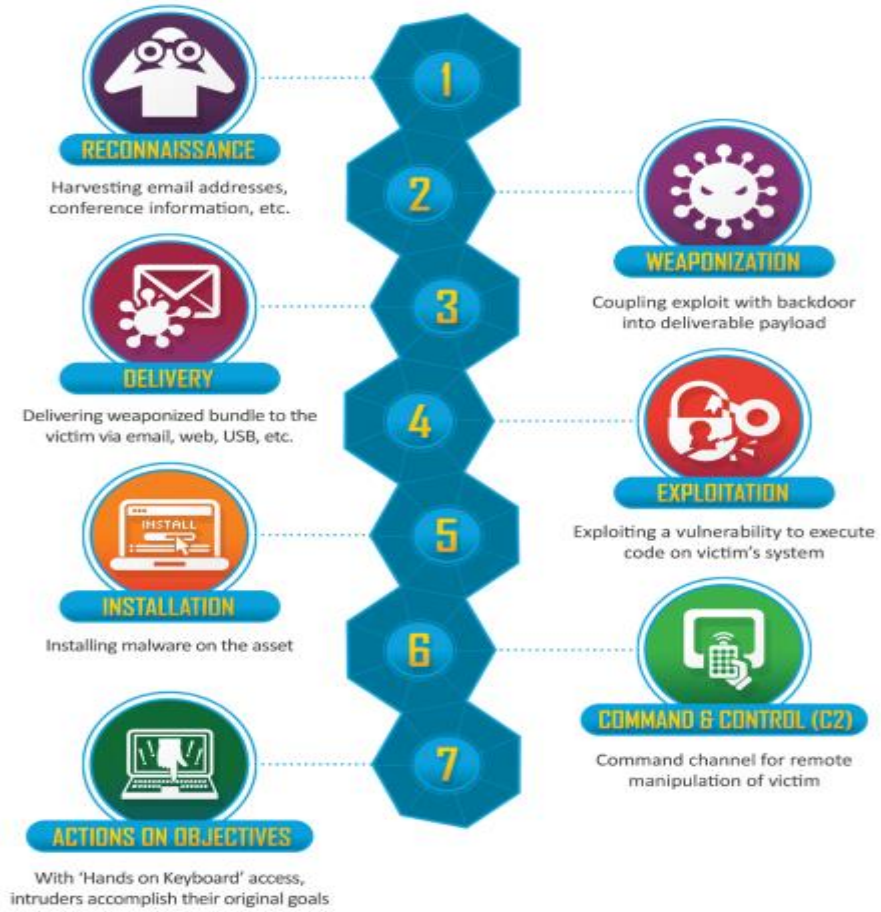
SECTION 3 : LA TARIFICATION

1 - CYBER KILL CHAIN

Issue du domaine militaire, l'expression "kill chain[1]", ou "chaîne cybercriminelle" désigne les étapes mises en œuvre par l'ennemi pour s'attaquer à une cible. En 2011, la société Lockheed Martin[2] a publié un document décrivant la "Cyber Kill Chain : CKC », s'inspirant du concept militaire. L'idée est d'appréhender chacune des phases afin de mieux détecter et contrer les attaques, plus l'ennemi est intercepté aux différentes étapes de la chaîne, moins il a de chances de parvenir à ses fins.

La CKC définit les sept stades d'une cyber-attaque, où chacune exige la réussite de la précédente.

Figure n° (II.27) : Chain kill cyber



[1] https://www.varonis.com/blog/cyber-kill-chain/
[2] http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

CHAPITRE II : LA CONCEPTION ET LA COMMERCIALISATION DU PRODUIT « ASSURANCE DES RISQUES CYBERNETIQUES »

Étant donné que chaque étape de la CKC dépend de l'échec de celle qui la précède, les incidents de cybersécurité peuvent être modélisés de façon stochastique par l'analyse de Markov.

Nous traiterons ici de l'application de l'analyse de Markov à la CKC comme moyen de quantifier la probabilité de défaillance d'un système de cybersécurité sur une période donnée ou un nombre d'attaques.

La CKC de Lockheed Martin expose l'ensemble d'étapes ou de stades que suit l'attaquant pour s'introduire dans un réseau informatique et l'exploiter.

Chaque stade du processus consolide le stade précédent ou en tire avantage. Toute rupture de la chaîne bloque l'attaquant. Les étapes ci-dessous décrivent la Cyber Kill Chain :

Reconnaissance : l'attaquant réunit des informations sur sa cible avant de passer à l'attaque. En effectuant des recherches sur des sites Internet, les cybercriminels essayent de collecter les adresses mail, les comptes rendus diffusés (des conférences, séminaires, formations…) et les relations via les réseaux sociaux. Forts de cette information, ils se préparent à passer à l'étape suivante.

Armement : le cybercriminel n'interagit pas avec la victime ciblée, mais met au point une arme d'attaque, il couple le logiciel malveillant à d'autres outils, tels qu'un document Word ou du contenu Adobe Flash. Une fois l'arme créée, la livraison peut avoir lieu.

Livraison **:** transmission de l'arme d'attaque aux victimes ciblées. Les trois vecteurs de livraison les plus répandus sont les pièces jointes, les sites Web et les supports amovibles USB.

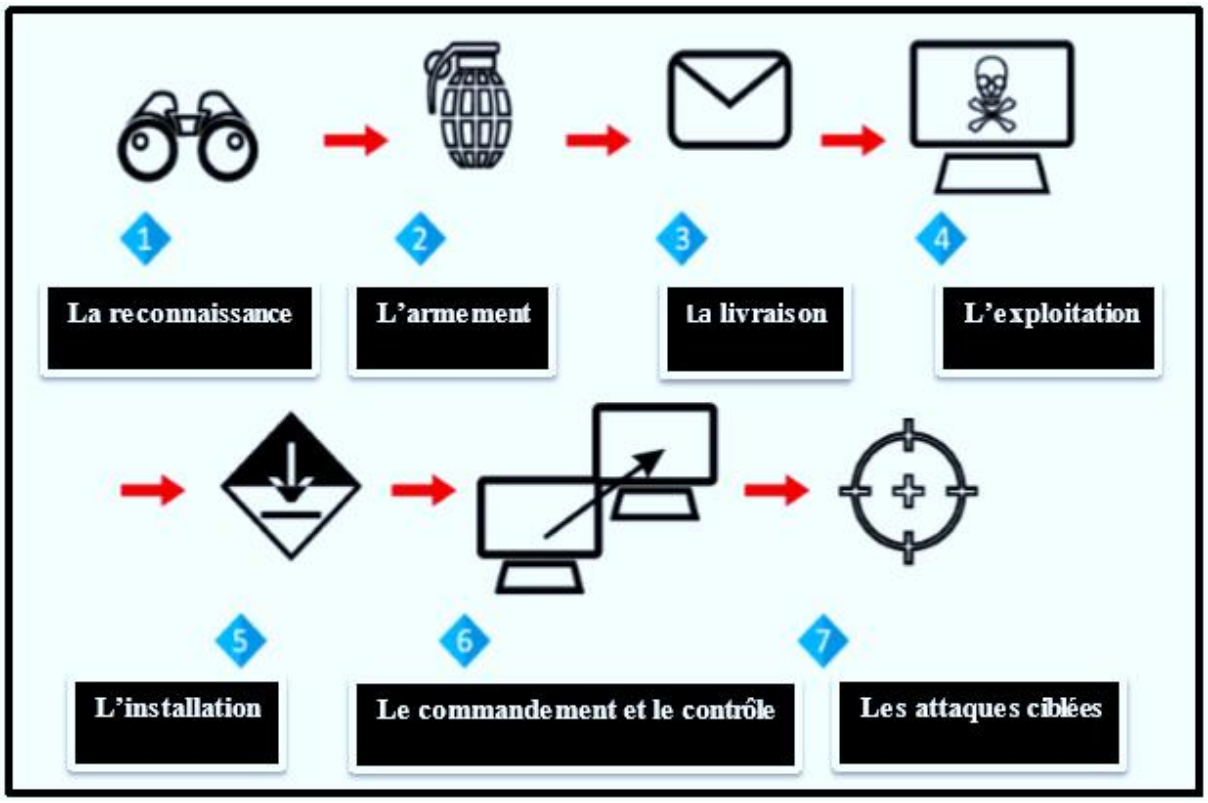
Exploitation *:* il s'agit du déclenchement proprement dit de l'attaque ; c'est le fait d'exploiter les vulnérabilités et de livrer le code malveillant sur le système afin de mieux s'implanter.

Installation : les intrus tentent d'avoir accès en installant dans le système un cheval de Troie ou une porte dérobée.

Commande et contrôle **:** une fois l'ordinateur compromis et/ou infecté, il doit se connecter à un système de commande et de contrôle pour que le cybercriminel puisse en prendre le contrôle.

Les attaques ciblées : ce n'est qu'après avoir franchi les six premières phases, que les intrus peuvent agir pour atteindre leurs objectifs. L'objectif en question est habituellement l'extraction de données, en passant par la collecte, le cryptage (Processus par lequel on rend la compréhension d'un document impossible en l'absence de la clef de chiffrement) et la récupération d'informations dans le milieu de la cible. Les intrus peuvent également utiliser la victime initiale pour accéder à d'autres victimes éventuelles au sein du réseau.

Figure n° (II.28) : schéma explicatif du la chaine cybercriminalité



Pour chaque étape, il existe des outils ou processus de sécurité de l'information pour détecter ou prévenir les intrusions. Peut estimer la probabilité de succès de l'attaquant et vice versa, la probabilité de défaillance de l'outil de sécurité

Bien que les deux phases de reconnaissance et d'armement soient effectuées en dehors du réseau informatique cible, la probabilité de succès ou d'échec peut être estimée. En fait, les systèmes de détection d'intrusion peuvent surveiller les scans de port pendant la phase de reconnaissance ou utiliser l'analyse Web pour déterminer si un attaquant collecte des informations.

2 - L'ANALYSE DE MARKOV : LE PRINCIPE SIMPLE

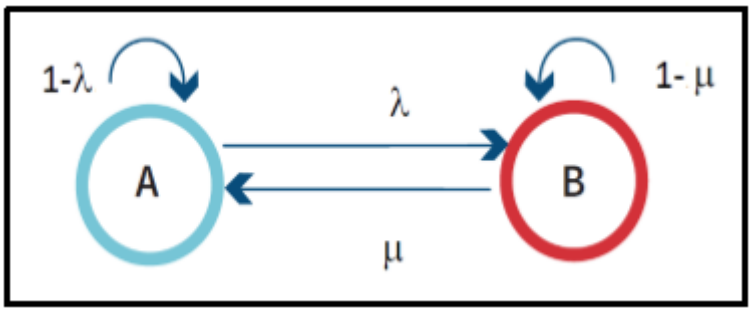
On a recours à l'analyse de Markov pour divers types de calculs de fiabilité, où une séquence d'événements dépendants peut conduire à des défaillances du système. Parmi les types de l'analyse de Markov, on trouve la chaîne de Markov.

[1]Il s'agit d'une méthode stochastique permettant de déterminer l'état probable d'un processus basé sur la probabilité d'événements, où chaque événement ne dépend que de celui qui le précède immédiatement. Par exemple, dans la CKC, le stade de l'exploitation n'a lieu que si le stade de la livraison a été réussi.

L'interdépendance des états peut être représentée par un diagramme de transition d'états, les états sont désignés par **A** et **B.**

La probabilité de passer de l'état **A** à l'état **B** est désignée par **λ** et la probabilité de revenir à l'état **A** à partir de l'état **B** est notée par **μ**. La probabilité de rester dans un état particulier est représentée par **1** moins la probabilité de sortir de l'état présent, c'est-à-dire la probabilité de rester dans l'état **A**, par exemple, est donnée par **1-λ**.

Figure n° (II.29) : diagramme de transition d'états de la chaine de Markov



Nous pouvons construire une matrice de transition à partir de ce diagramme la probabilité de rester dans l'état A est donnée par 1- λ (c'est-à-dire de passer de l'état A à l'état A). Comme nous l'avons vu, la probabilité de passer de l'état A à l'état B est désignée par λ. La matrice de transition, pour un cas simple constitué de deux états s'écrit de la sorte :

$$\begin{matrix} 1-\lambda & \lambda \\ \mu & 1-\mu \end{matrix}$$

[1] JRMS_cybersecurity_essays

$1 - \lambda$: La probabilité de rester dans l'état A ;

λ : La probabilité de passage de l'état A à l'état B ;

μ : La probabilité revenir à l'état A à partir de l'état B ;

$1 - \mu$: La probabilité de resterà l'état B.

Suite à une succession de passage par plusieurs états, la probabilité d'être dans un certain état après un certain nombre de cycles peut être représentée par l'équation suivante :

$$xt = x0 \times Pt$$

Avec :

x : est le vecteur d'état du système ;

$x0$: est le vecteur d'état initial du système ;

P : La matrice de transition.

3 - CALCUL DE LA PROBABILITÉ D'UNE FAILLE DE CYBERSÉCURITÉ : APPLICATION DE LA CHAINE DE MARKOV AU CYBER KILL CHAIN :

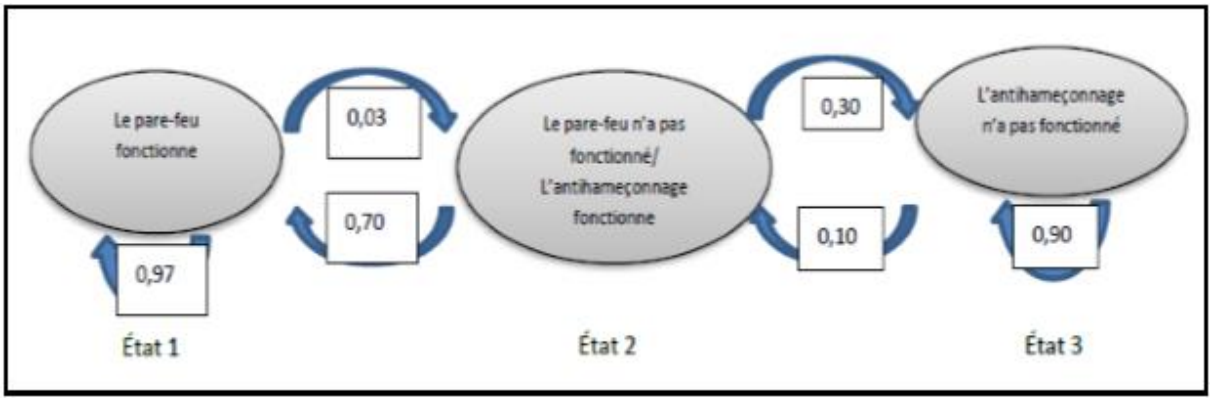
L'application de la chaîne de Markov à la CKC permet de calculer la probabilité de défaillance d'un système de cybersécurité. Par la suite, nous utiliserons un simple exemple et des probabilités statiques.

La probabilité de rester dans un stade de la CKC est liée aux mécanismes de prévention, tandis que les mécanismes de détection et de correction sont regroupés pour calculer la probabilité de revenir à un stade précédent.

Ainsi, la correction d'une faiblesse dans un système d'exploitation se fait à travers un mécanisme correctif. Afin de simplifier la compréhension de ce principe, on va se limiter à examiner deux stades. L'exemple suivant définit la chaîne de Markov de la CKC pour le passage [1]de l'état (1) à l'état (3) en utilisant les deux étapes suivantes : livraison et exploitation.

[1]http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Figure n° (II.30) : Diagramme de transition de CKC



- Dans ***l'état 1***, la prévention de la livraison fonctionne (c'est-à-dire que le pare-feu bloque les pourriels selon un taux de 97 %) ;
- Dans ***l'état 2***, la prévention de la livraison a échoué et la prévention de l'exploitation fonctionne (c'est-à-dire que les utilisateurs ont appris à ne pas ouvrir de pièces jointes selon un taux de 70 % et ils rapportent l'existence du courriel) ;
- Dans ***l'état 3***, la prévention de l'exploitation a échoué. Pour cet exemple, il y a une faible probabilité que l'exploitation soit détectée par d'autres outils (10 %) et la chaîne revient à l'état 2 ;

La figure illustre la probabilité de ces états à l'aide d'un diagramme de transition, Selon ces probabilités, nous obtenons la matrice de transition suivante :

$$P = \begin{pmatrix} 0.97 & 0.03 & 0 \\ 0.7 & 0 & 0.3 \\ 0 & 0.1 & 0.9 \end{pmatrix}$$

Les lignes représentent les états actuels et les colonnes, les états où on peut aller.

- Le vecteur d'état initial est donné par $x0 = [1\ 0\ 0]$;
- Après 100 cycles (transition), le vecteur résultant est **x100** = [0,853 0,036 0,109] ;
- La probabilité que le logiciel malveillant soit exécuté est d'environ **11 %** (cela signifie que la probabilité d'être dans l'état 3 est de 0,109).

Avec le modèle CKC, nous pouvons regrouper les différents outils et processus utilisés dans la cybersécurité en une séquence logique. En établissant cette séquence logique, l'analyse stochastique de la fiabilité peut servir à calculer la probabilité de défaillance.

- Dans l'exemple précédent, le modèle utilisé était plutôt simpliste avec des probabilités statiques. Cependant, une fois que nous aurons une meilleure compréhension des taux de fiabilité des différents outils de sécurité, nous emploierons des probabilités plus complexes et plus rigoureuses. Cette compréhension des taux de fiabilité des outils de la cybersécurité dépend fortement de l'échange de données sur les menaces informatiques entre les entreprises. Fort heureusement, les entreprises divulguent de plus en plus ce genre d'informations.

De ce qui précède, on peut conclure que l'application d'une méthodologie de calcul de la fiabilité aux systèmes de cybersécurité peut aider à quantifier la probabilité de défaillance d'un système de cyber-protection. À partir du moment où la probabilité de défaillance est calculée, l'analyse actuarielle appliquée aux produits d'assurance est applicable aux systèmes informatiques.

4 - ÉTUDE DE CAS : UN CAS DE TARIFICATION POUR UNE BANQUE X

4.1 - Chronologie :

Le 1er décembre 2015, le logiciel de gestion de la banque X cesse brutalement de fonctionner. Leurs utilisateurs sont dans l'incapacité de trouver les clés de chiffrement permettant d'accéder aux données stockées.

Rançongiciel (Ransomware) : le 5 décembre 2015, un message est envoyé à cette banque en demandant une rançon pour la libération de ses données.

Le montant de la rançon est fixé à **20MDA** pour un retour des clés de chiffrement utilisées. La banque X tentera de payer la rançon pour se rendre compte que les moyens de communication fournis par l'attaquant sont inopérants.

Pour la banque X, elle était touchée par une semaine d'arrêt de commercialisation soit 30%

4.2 - Description :

L'attaquant a utilisé une faille de configuration de logiciel de gestion de la banque afin d'y accéder via un accès distant de maintenance. En utilisant cet accès, il active une fonction native du système permettant de chiffrer les données de celui-ci.

Utilisation d'un défaut de configuration de logiciel imputé à un défaut d'installation et d'exploitation (l'installation et l'exploitation de ce logiciel sont externalisées à un cabinet étranger)

4.3 - Conséquences dommageables :

- 1 semaine d'arrêt de commercialisation, 30% de baisse de rendement de commercialisation pendant une semaine ;
- Perte de la quasi-totalité des données gérées par le logiciel de gestion de la banque (noms des clients, numéro de comptes et carte bancaire, solde…) et notamment de commercialisation sur la période manquante, vu que la banque X ne dispose d'aucun Data center[1], toutefois certaines informations papiers restent disponibles.

4.4 - Autres conséquences dommageables

- Rançons ;
- Frais de reconstitution de données / assistance informatique ;
- Dépenses pour reprendre l'activité.

4.5 - Les couvertures proposées :

La banque ne dispose d'aucune assurance cyber risque, nous proposons donc un paquet de garantie

- Pertes d'exploitation ;
- Frais de gestion de crise ;

[1] Data center : un centre de données ou centre informatique est un lieu ou un service regroupant des équipements constituants du système d'information d'une ou plusieurs entreprises il peut être interne ou externe de l'entreprise

- Divulgation de données ;
- Paiement de la rançon « Cybercriminalité » ;
- Réparation de l'image de la banque ;
- RC utilisation frauduleuse des données de la clientèle.

4.6 - Limites des garanties (proposés par la banque X)+ Taux de la prime en fonction de cette limite :

GARANTIES	LIMITES	TAUX
Pertes d'exploitation	DE 10MDA à 30MDA	DE 0,5% à 5%
Frais de gestion de crise	DE 10MDA à 30MDA	DE 0,5% à 5%
Divulgation de données ;	DE 10MDA à 50MDA	DE 0,5% à 5%
Cybercriminalité	DE 5MDA à 7MDA	DE 0,5% à 5%
Réparation de l'image de la banque	---	---

CONCLUSION

Cet exemple a pour but de présenter et de mettre l'accent sur la gravité de risques cyber pouvant être causés à une entreprise et les garanties applicables pour se prémunir dans le proche futur. L'infection d'une entreprise par un virus informatique peut aisément se propager à une autre par le biais de ces interconnections. La sécurité informatique mise en place par chacune d'elles est cruciale mais ne peut garantir une protection infaillible. À l'aide de l'application de la chaîne de Markov à la chaîne de la cybercriminalité, nous avons constaté que la probabilité d'une attaque informatique réussie peut atteindre 10,9%.

C'est ainsi le rôle des compagnies d'assurances algériennes et de réassurances pour développer ce nouveau produit, Le risque Cyber peut s'apparenter à un risque Catastrophe, que les assureurs et les réassureurs connaissent paradoxalement plutôt bien.

Par conséquent, ils doivent poursuivre la formation, l'information, l'investissement, la prise de conscience de tous les acteurs face au risque cyber et son caractère systémique, Le développement de couvertures d'assurance qui reconnaitront l'effort de connaissance en interne du niveau d'exposition au risque cyber, définir les cyber-incidents afin que les clauses du

contrat d'assurance soient robustes et reconnues par l'ensemble des parties prenantes, afin d'améliorer la clarté et la robustesse du contrat.

CONCLUSION GÉNERALE

CONCLUSION GÉNÉRALE

Au cours de nos développements, nous avons pu découvrir que face à l'intensification tant en volume qu'en technicité des menaces de type informatique et numérique, c'est-à-dire les « Cyber-risques », les assureurs ont entrepris de mettre en place des couvertures d'assurance adaptée à ce nouveau risque.

En outre, les Cyber-risque ont notamment pour effet de porter atteinte lorsqu'ils se réalisent aux intérêts pécuniaires et financiers de sa victime. Dès lors, c'est naturellement que les assureurs ont mis au point des assurances dites de dommages, c'est-à-dire des assurances ayant pour vocation de protéger les intérêts économiques de l'assuré.

Si tout utilisateur, exploitant ou responsable du traitement de données numérique peut désormais bénéficier d'une assurance efficace et adapté à un risque bien particulier, il n'en demeure pas moins que toute son attention doit être requise lors de la souscription d'un tel contrat. En effet, comme nous l'avons développé, il réside un certain risque, en ce que l'assuré est toujours couvert par d'autres contrats qui préexistent à l'assurance contre les risques Cyber. Dès lors, cette nouvelle police ne doit pas devenir l'occasion pour l'assurer de souscrire de nouvelles garanties, au demeurant, relativement onéreuses, pour des risques contre lesquels il est finalement déjà couvert. Ce cumul d'assurance place alors l'assuré dans une situation délicate puisque ce dernier paie pour un service qui ne pourra peut-être pas lui être fourni en raison du principe d'indemnitaire.

L'étude des Cyber-risques, constitue, une tâche principalement à destination des services d'assurance des risques d'exploitation de toute entreprise qui souhaite se prémunir contre ce type de risque. En effet, il revient à chaque entité d'identifier et quantifier son potentiel de risque afin de prendre toutes les mesures nécessaires et adéquates. S'agissant des risque Cyber, ce dernier étant relativement récent et les outils assurantiels mis à disposition par les assureurs l'étant encore.

Nous avons, dans un premier temps, permis au lecteur de se familiariser avec les spécificités du cyber-risque. Nous avons présenté le vocabulaire technique et métier, le marché des risques cyber, l'évolution de la demande de la cyberassurance, et une enquête de ce nouveau produit et de son statut pour les banques. Cela permettra au lecteur voulant approfondir le sujet d'avoir les bases lui permettant de faire des études plus poussées.

CONCLUSION GÉNÉRALE

Un souscripteur peut donc trouver dans ce mémoire le vocabulaire lui permettant de communiquer avec son client ainsi que trouver les indicateurs qui pourraient lui permettre de se faire un meilleur avis du risque assuré. L'actuaire trouvera des présentations techniques pour l'aider à continuer ses études et établira un modèle de tarification bien précis. Enfin, l'assureur pourra trouver des informations sur le marché mondial ainsi que les statistiques dont il pourrait avoir besoin sur ce marché.

D'autre part, nous avons observé que l'exploitation des commentaires à l'aide de l'enquête nous apporte des informations utiles. En particulier, nous avons trouvé quelques indications sur la durée nécessaire à la reprise de l'activité après une attaque cyber, l'intention de signer un nouveau contrat de cyberassurance, la limite de garantie exigée par les banques... De plus, un modèle est construit sur une étude stochastique permet de calculer la probabilité de défaillance d'un système d'information mais dans le contexte actuel d'absence de données et de statistiques significatives, avec étude de cas d'une banque victime d'une cyberattaque et ses conséquences destructrices.

Enfin, nous espérons qu'à travers ce travail, basé sur des données statistiques du monde entier, en sélectionnant comme échantillon le secteur bancaire qui constitue la cible du cyber-incident, nous mettrons en évidence la gravité du cyber-risque en Algérie.

Ce travail sera le point de départ d'une série d'études sur l'assurabilité des risques cybernétiques en Algérie et demain sera peut-être le début des changements du cadre réglementaire et de l'obligation de l'entreprise de divulguer des informations claires et précises décrivant les attaques et les erreurs informatiques dont elles étaient victimes ; et l'élaboration d'un modèle de tarification sera une tâche possible et réalisable.

Par conséquent, le développement de ce produit est désormais entre les mains des compagnies d'assurance et de réassurance algériennes, et de mettre des programmes de cyberassurance forment une réponse adaptée au risque cyber parce qu'ils couvrent les dommages subis par l'assuré et les dommages subis par les tiers, tout en fournissant à l'assuré des prestations d'assistance et de gestion de crise. Les assurances traditionnelles n'apportent pas une telle réponse à ce risque parce qu'aucune d'entre elles n'est d'une nature mixte.

CONCLUSION GÉNÉRALE

RECOMMANDATIONS

- ✓ L'Algérie ne dispose pas encore d'offre « cyber risque », un nouveau mode de distribution des produits cyber pourrait être également prévu afin de participer à la création et au développement du marché des assurances cyber, à l'aide de partenariat avec les fournisseurs de matériel informatique, qui, proposeraient à leurs clients une assurance cyber lors de l'achat du produit.

- ✓ Au-delà du ciblage de la clientèle, les assureurs doivent adopter une logique de Servicing pour les clients voulant s'assurer contre le risque cyber. En effet, ceux-ci n'ont pas seulement besoin d'indemnisation, mais également d'un accompagnement pour prévenir et gérer la situation délicate d'une attaque cyber.

- ✓ La sensibilisation des clients est aussi un point clé de l'évolution de l'offre, à travers des sessions de e-learning, des audits préventifs, avec une communication différenciée selon les segments.

- ✓ L'assureur n'est donc plus qu'un simple assureur dans ce domaine, mais également un prestataire de service de prévention et de gestion de risque.

- ✓ Enfin, la progression du marché de la cyberassurance en Algérie dépend à la fois des assureurs et des réassureurs : tant qu'il n'y aura pas d'offres matures de réassurance dans le domaine, les assureurs ne pourront pas se développer à grande échelle.

BIBLIOGRAPHIE

Ouvrages :

1.« Americans and Cybersecurity » Pew Research Center, January 26, 2017.

2.« Baromètre de la cybersécurité des entreprises », Cesin - Opinion Way, janvier 2019.

3.Philippe MALAURIE, Laurent AYNES, Philippe STOFFEL-MUNK. « Droit des obligations ». 7ème Edition. LGDJ, Lextenso édition. 2016

Revues :

1.Ronald Chidiac, CEO de BROKTECH SAL, Revue de L'ASSURANCE N°19 - Décembre 2017.

2. Argus de l'assurance. N° 7466 – 7467. 15 juillet 2016

3. Argus de l'assurance N°7466 – 7464. 1er juillet 2016

4. Atout Risk Manager, La revue des professionnels du risque et de l'assurance n° 7 Trimestriel. Décembre 2015

Articles :

1.Arnaud TESSALONIKOS. « 3 Question : Entreprise et prévention des risques numériques ».

2.La semaine juridique Entreprise et Affaires n°47. 19 novembre 2015

3.Éric. A. CAPRIOLI. « Les notifications des données à caractère personnel et le droit : des questions en suspens ». Communication, commerce électronique n°5. Mai 2010.

4.Daniel. LANGE. « Intermédiaires d'assurance – règles particulières aux courtiers ». Jurisclasseur. Fasc. 640. 16 Février 2016.

5.« INFORMATIQUE. – Données à caractère personnel. – Introduction générale et champ d'application de la loi "Informatique et libertés". Juris Classeur Administratif. Fasc. 274-10. 30 juillet 2014.

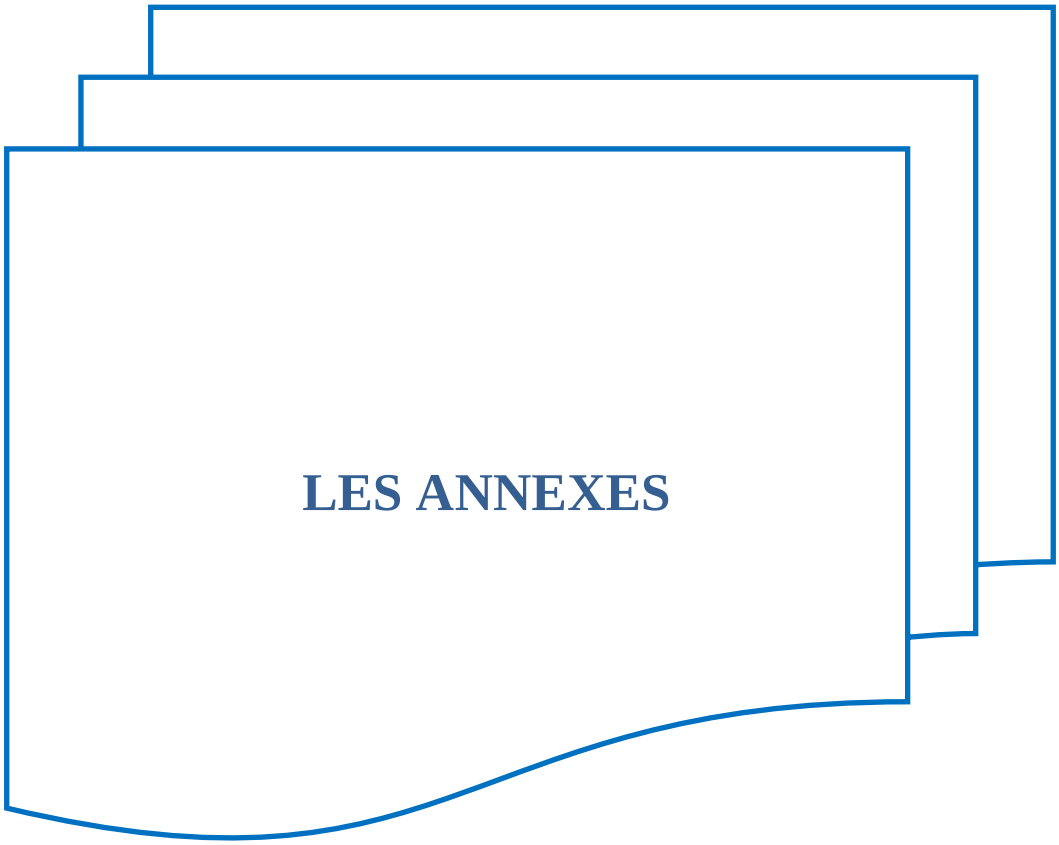
Mémoires :

1.Master professionnel Sciences de gestion, mention finances des marchés Spécialité Actuariat du CNAM, 2015.

2.Mémoire « **assurance des risques cybernétiques** » ; Abbes Yosra ; 2018 ; p27

Sitographie :

1. https://www.atlas-mag.net/article/le-marche-de-la-cyberassurance-en-2019
2. https://www.finextra.com/blogposting/15278/cyber-insurance-pricing-quantifying-the-unknown-in-a-multibillion
3. https://www.algiersherald.com/cybersecurity-in-algeria/
4. https://www.osac.gov/Country/Algeria/Content/Detail/Report/aceef5ea-f045-453b-8fc9
5. https://www.aigassurance.fr/cyberedge.SUISSERE
6. https://www.varonis.com/blog/cyber-kill-chain/
7. http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
8. http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
9. https://www.atlas-mag.net/article/cyberattaques-des-chiffres-qui-inquietent-assureurs-et-reassureurs



LES ANNEXES

Annexe 01 : Le questionnaire

QUESTIONNAIRE

Madame, Monsieur, étudiante en Assurance à l'Institut de Financement du Développement du Maghreb I.FI.D, je réalise un mémoire de fin d'études sur l'ASSURANCE DES RISQUES CYBERNETIQUES pour les banques algériennes vu l'émergence de ces risques durant les dernières années. Je vous remercie de bien vouloir consacrer une partie de votre temps pour répondre au questionnaire ci-joint

Vos réponses sont anonymes

Structure du questionnaire :

Section A : Informations générales

Section B : Sécurité de système d'information

Section C : Risques cybernétiques

Section D : Assurance des risques cybernétiques

1. **Informations générales :**

- Veuillez évaluer les facteurs qui entraînent un changement important du niveau de risque cybernétique au cours des dix dernières années

  ☐Développement de l'internet des objets
  ☐Accumulation des méga données
  ☐Ouverture de l'infrastructure Cloud au grand public
  ☐Le niveau d'externalisation

- Considérez-vous que votre organisme est menacé par des cyber-attaques ?
  ☐Oui
  ☐Non

  Si oui, veuillez évaluer le niveau de risque perçu
  ☐Important
  ☐Modéré
  ☐Faible

- Avez-vous un site web de commerce ou de service en ligne ?
  ☐Oui
  ☐Non

Si oui, quelle est la part de revenu généré ou supporté par le site web ?(estimation)

2. **Sécurité de système d'information :**

L'accès aux systèmes d'information exige l'identification et l'authentification des utilisateurs, et la gestion du renouvellement et du durcissement des mots de passe est mise en place ?	☐Oui ☐Non
Une segmentation du réseau est mis en place pour séparer les zones critiques (serveurs, administration..) des zones moins critiques (zone bureautique)	☐Oui ☐Non
Un antivirus est installé sur tous les systèmes et les mises à jour antivirus sont supervisée ?	☐Oui ☐Non
Effectuez-vous régulièrement des audits de vulnérabilité et/ou des tests d'intrusion ?	☐Oui ☐Non
Votre entreprise dispose t'elle d', au moins, un expert en sécurité informatique et protection des données ?	☐Oui ☐Non
Avez-vous mis en place une procédure de notification aux individus et au régulateur en cas de violation des données ?	☐Oui ☐Non
Est-ce que l'ensemble du personnel reçoit une formation ou une sensibilisation aux risques cyber et aux bonnes pratiques de l'hygiène de sécurité informatique ?	☐Oui ☐Non

3. **Risques cybernétiques**

Avez-vous été victime d'une attaque Cyber ou d'une erreur informatique ?	☐Oui ☐Non ☐Je ne peux pas répondre
Si oui, quelles ont été les conséquences de cette attaque/erreur ?	☐Perte ou usurpation de données confidentielles ☐Pertes d'exploitation ☐Vol de propriété intellectuelle ☐Atteinte à la réputation

Si oui, comment /combien quantifiez-vous la perte ?	☐Non déclarée ☐Pas de perte ☐Modéré ☐Importante
Des mesures ont-elles été prises pour éviter le renouvellement des sinistres de même nature que ceux déjà survenus ?	☐Oui ☐Non
Le délai nécessaire à la reprise d'activité en cas d'incident sur vos systèmes d'information est-il estimé à plus de 12h ? (Si oui combien du temps ?)	☐Oui ☐Non ……..
Pensez-vous que les risques cyber ont évolué, plutôt, en termes de fréquence ou de sévérité ?	☐Fréquence ☐Sévérité ☐Les deux

4. L'assurance des risques cybernétiques :

- Avec la révolution numérique et digitale en Algérie, prévoyez-vous de souscrire une assurance cybernétique pour faire face aux coûts inhérents à une erreur ou une attaque cyber ?

  ☐Oui

  ☐Non

  ☐C'est trop tôt pour y penser

Si oui, quelles sont les couvertures que vous jugez utiles ?

COUVERTURE DIRECTE		SEVERITE	LIMITE DE COUVERTURE(DA)
Gestion des crises	☐Oui ☐Non	☐Forte ☐Moyenne ☐Faible	
Perte d'exploitation	☐Oui ☐Non	☐Forte ☐Moyenne ☐Faible	
Protection de la base de données	☐Oui ☐Non	☐Forte ☐Moyenne ☐Faible	
Divulgation des données	☐Oui ☐Non	☐Forte ☐Moyenne ☐Faible	
Fraude	☐Oui ☐Non	☐Forte ☐Moyenne ☐Faible	

Propriété intellectuelle	☐Oui ☐Non	☐Forte ☐Moyenne ☐Faible	
Cybercriminalité	☐Oui ☐Non	☐Forte ☐Moyenne ☐Faible	
Détournement de fonds	☐Oui ☐Non	☐Forte ☐Moyenne ☐Faible	
Accès non autorisé	☐Oui ☐Non	☐Forte ☐Moyenne ☐Faible	
Utilisation des licences piratées	☐Oui ☐Non	☐Forte ☐Moyenne ☐Faible	

Annexe 02 : violation des données 2014-2015

ENTREPRISES	DONNÉES DÉROBÉES	TYPE DE DONNÉES
PREMERA BLUE CROSS Date d'annonce : 18 mars 2015	11 M	Numéro de compte bancaire Numéro de sécurité sociale
ANTHEM Date d'annonce : 05 février 2015	80 M	Numéro de sécurité sociale Adresses email Adresses physique
SONY Date d'annonce : 25 novembre 2014	47 000	Information de l'entreprise Données d'employés
HOME DEPOT Date d'annonce : 02 septembre 2014	109 M	Numéro de carte de crédits Adresse email
JP MORGAN Date d'annonce : 27 aout 2015	83 M	Adresses email Adresses physique
Ebay Date d'annonce : 21mai 2014	145 M	Adresses email Adresses physique Identification de connexion
TARGET Date d'annonce : 13 décembre 2013	110 M	Numéro de carte de crédits
ADOBE	2014	150 M

Annexe 03 : Les risque cyber d'origine malveillant/ criminel

Nation 	• Economique, politique, etmilitaire	• Secrets, brevets, • Informationsensible, • Technologiquenou velle/émergente • Infrastructurecritique • Carence de fournisseur(s) stratégique(s)	▶ Perte d'avantage et de compétitivité, ▶ Perturbation d'infrastructurescritiques ▶ Conflits politiques/diplomatiques
Organisation criminelle 	• Gain financier immédiat • Collected'informatio ns pour de futursgains financiers	• Systèmes de règlement financiers/de paiement/ Serveur Terminal Caisses • PCI (« Payment Card Information») • Information employésidentifiable • Information / données clients, cartesbancaires	▶ Enquêtes et sanctions réglementairescoûteuses ▶ Poursuitesengagés par les clients etactionnaires ▶ Perte de confiance du consommateur
Organisation Terroriste 	• Politique, idéologique ou religieuses afin d'entrainer une désorganisationgénér ale et susceptible de créer la peur et lapanique	• Tout systèmed'informations : les media, les entreprises, les sites gouvernementaux, les systèmes SCADA, les particuliers	▶ Menace la paix et la sécurité et de la sureténationale par des actions ayant pour conséquencedes: • dommagesmatériels • atteintes auxpersonnes
Hacktiviste 	• Influence politique et/ou au changement social/sociétale • Pression sur les entreprisespour changer leur pratiques	• Secret industriel oucommerciaux • Information commercialesensible/ politique des prix/référencesfournisseurs • Informationsrelatives aux principaux dirigeants, personnel, clients et partenaires	▶ Perturbation des activités de l'entreprise, perte demarché ▶ Marque etréputation ▶ Perte de confiance du consommateur
Insiders Initiés 	• Avantage personnel, gainfinancier • Vengeance professionnelle • Patriotisme	• Ventes, offres, marchésstratégiques • Secret industriels et commerciaux y compris des partenaires, et dans unemoindremesure brevet,R&D, • Opération, stratégiecommerciale • Informationpersonnel	▶ Divulgation de secrets professionnels,brevets, ▶ Perturbation desopérations, ▶ Marque etréputation, ▶ Impact sur lasécurité

Annexe 04: Les risques cyber d'origine accidentelle

Incidents accidentels	Nature de l'évènement	Conséquences	Impacts financiers
Erreur humaine 	• Erreur de programmation, • Erreur d'implémentation, • Erreur d'utilisation, • Erreur de maintenance	▶ Arrêt des systèmes d'informations ▶ Responsabilité en cas d'erreur opération client, délivrance de bien ou services, ▶ Perte ou altération de données client, de Données confidentielles, ou de données d'exploitation ▶ Procédure réglementaire	▶ Frais supplémentaires d'exploitation ▶ Frais de défense / Dommages et intérêts ▶ Frais de reconstitution de données ▶ Pertes d'exploitation ▶ Cout du matériel de remplacement ▶ Frais et sanction administrative
Panne/problèmes techniques 	• Défaut de maintenance • Problème de mise en production d'un logiciel • Problème d'interopérabilité des systèmes avec fournisseurs, tiers, client • D'origine industrielle électrique : commutation de contacts, fonctionnement de thyristors, etc. • Electronique : réseau de distribution, problème de relais,		
Evènement naturel 	• Incendie, • Inondation, • Dégât des eaux • Tempête • Foudre et surtension électriques liées		

Annexe 05 : Description des dommages subis par l'entreprise

Pertessubies	Impacts financiers potentiels
Pertesoudommages aux données	Perteoudétérioration de donnéesou de logiciels, entrainant des coûts de restauration, de mise à jour, de reconstitution ou de remplacement de cesactifs

Interruption d'activité ouindisponibilité duréseau	Perted'exploitationencasd'interruption, dégradation du service ouralentissement du réseau, qui entraînentuneperte de revenus, une augmentation des coûts de fonctionnement et/ou des frais d'atténuation etd'investigation
Atteinte à la réputation	Découlantd'une violation de la protection des données qui entraîneuneperte de la propriétéintellectuelle, uneperte de revenus, uneperte de marché
Investigation par le régulateur sur le non-respect de la vieprivée	Enquête, procédureréglementaire (CNIL) ; frais de défense, amendesrésultantd'uneenquêteoud'exécutiond'unerégulateuren raison de la sécurité et de la responsabilité de la vie privée
Frais de notification	Frais juridique, frais de poste et de communication dans les pays où il y a une obligation légaleouréglementaired'informer les individusd'une violation de sécuritéou de confidentialité, y compris les frais de réputationliés

Annexe 06 : Top 10 des cyberattaques en 2018

Rang	Cyberattaque	Sociétés attaquées	Période	Nombre de données piratées	Type de données piratées
1.	**Aadhaar ***	**Unique Identification Authority of India (UIDAI)**: organisme relevant du Ministère de l'électronique et des technologies de l'information	Mai	1 100 000 000	Données personnelles des clients
2.	**Marriott**	**Starwood**: filiale du groupe hôtelier mondial Marriott.	Septembre 2018 (pourrait remonter à 2014)	500 000 000	Données personnelles et bancaires des clients
3.	**Exactis**	**Exactis**: société américaine de marketing	Juin	340 000 000	Données personnelles des clients
4.	**MyFitnessPal**	**Under Armour**: société américaine spécialisée dans la fabrication des chaussures et vêtements de sport	Février	150 000 000	Données personnelles des clients

5.	**MyHeritage**	**MyHeritage**: plateforme internationale de généalogie en ligne	Juin	92 000 000	Données personnelles des clients
6.	**Panera Bread**	**Panera Bread**: chaîne américaine de boulangeries et de cafés	Aout 2017 – Avril 2018	37 000 000	Données personnelles des clients et les quatre derniers chiffres des cartes bancaires
7.	**Facebook**	**Facebook**: société américaine propriétaire du réseau social au même nom	Septembre	30 000 000	Données personnelles des clients
8.	**TicketFly**	**TicketFly**: site de distribution de billets au Canada et aux Etats-Unis	Mai	26 151 608	données personnelles des clients
9.	**Sacramento Bee**	**The Sacramento Bee**: quotidien californien	Janvier	19 500 000	Données des électeurs en Californie
10.	**PumpUp**	**PumpUp**: société spécialisée dans le domaine du sport et fitness, basée à Ontario au Canada	Mai	6 000 000	Données personnelles et bancaires des clients

Annexe 06 : exemples des risques cyber et leur cout moyen

Risque cyber	Exemple	Coût moyen
Phishing	Un faux e-mail de banque.	NC
Ransomwares	Un fichier téléchargé sur internet contient un virus *ransomware*.	15 000 €
Dommages aux biens	La détérioration de matériel informatique suite à une panne.	Entre 30 et 60 € pour la suppression de virus 100 € pour la récupération de données Entre 80 et 100 € pour le remplacement de la carte mère Coût moyen : 50 €/h
Fraude téléphonique	Un numéro payant appelle en demandant de le rappeler par la suite.	Surfacturation du type 3 € par appel + 3 € la minute par un numéro qui force à le rappeler
Atteinte à l'image	Faux compte de réseau social avec la photo de la victime.	2 229 € en moyenne pour une usurpation d'identité sur internet
Réputation sur internet	Photos compromettantes sur les réseaux sociaux.	Minimum 100 € pour la suppression d'un lien (entre 100 et 200 €/h)
Détournement de fonds	Utilisation frauduleuse du compte bancaire internet.	75 € en moyenne : 440 millions € pour la fraude à la carte bancaire en 2018 pour 6 millions de fraude (Observatoire de la sécurité des moyens de paiement)
Perte de données personnelles	Défaillance du système de Cloud.	NC

TABLE DES MATIÉRES