Table des matières

Contenu

Table de figures

Liste des tableaux

Introduction générale

Dès sa naissance, l'assurance a poussé à la limitation des risques. Cette tendance est particulièrement observable dans le cas des développements de l'assurance dans tous les domaines. Les assurances classiques comme la couverture contre l'incendie et les pertes d'exploitation offrent des garanties financières au client en cas de sinistre matériel affectant le patrimoine propre. Les assurances de responsabilité permettent quant à elles de dédommager des tiers ayant souffert d'un préjudice lié à une faute du preneur d'assurance. Ces polices traditionnelles datent toutefois de l'ère « pré- numérique » et concernent principalement les dommages matériels et corporels.

Les pertes financières associées à la perte de connexions de données ou de connexions réseau ne sont donc pas totalement couvertes par ces assurances classiques. Le besoin d'une solution d'assurance concluante se fait par conséquent sentir. Les cyberrisques constituent un élément majeur des risques opérationnels et tant les entreprises que les particuliers se tournent vers l'industrie de l'assurance pour obtenir une protection contre ceux-ci.

Dès lors qu'un petit cyber-escroc peut empocher plusieurs milliers de dollars par jour sans être inquiété ou repéré par l'administration ou les autorités judiciaires de son pays. Pour l'heure, les cybercriminels n'ont d'autre objectif que de gagner de l'argent - et beaucoup d'argent. Virus, spams et autres ont beau drainer plusieurs centaines de millions de dollars chaque année à travers le monde, l'existence d'un véritable cadre politique international permettant la définition de mesures efficaces de lutte contre la cybercriminalité continue de manquer.

Les cybercriminels innovent constamment, non seulement ils font un usage intense des médias sociaux pour escroquer les utilisateurs et distribuer des liens à des logiciels malveillants, mais ils parcourent aussi l'environnement pour identifier les nouvelles vulnérabilités, les nouveaux environnements populaires auprès des internautes et les nouveaux vecteurs d'attaques. Ces dernières années ont été marquées par de nombreuses Cyberattaques qui mettent en évidence la réalité, la diversité et la matérialité des risques Cyber qui sont maintenant devenus un sujet de préoccupation des directions générales et des autorités de régulation. Par conséquent, l'assurance Cyber est en forte croissance, tant chez les assureurs avec le développement de l'offre que chez les clients qui sont de plus en plus nombreux à souscrire cette garantie en complément des mesures de prévention et protection.

L’assurance cyber trouve ses origines dans les années 1980 avec l’arrivée des premiers réseaux informatiques. L’offre de cyber assurance a commencé dans les années 1990 avec internet et le risque d’attaque à distance, la fraude et les erreurs technologiques. Après presque 30 ans d’existence c’est encore un risque jeune et en plein développement.

La couverture proposée par une assurance cyber peut couvrir des risques très divers :

- Les frais liés à la recherche et à la résolution de la faille
- La perte d’argent causée par l’attaque ou l’erreur commise
- Les dommages occasionnés par la divulgation ou la menace de révéler des informations personnelles etc...

Dans la première partie de ce rapport, on va établir un aperçu général sur la situation du marché cyber à l’échelle mondial puis à l’échelle national en se focalisant sur l’évolution des risques cybernétiques et de l’assurance cyber en parallèle.

La deuxième partie du travail va porter principalement sur la conception et la création d’un produit assurance des risques cybernétiques adapté aux besoins du 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 1 : L'assurabilité des risques cybernétiques : Etat des lieux

Introduction

Depuis quelques années, l'activité des cybercriminels est de plus en plus effrénée. Et ceci a pour cause l'avancement de l'internet a pas de géant chaque jour et le nombre d'internautes qui ne cesse de grandir, a cela s'ajoute l'évolution du e-business. Un cocktail explosif qui a touché tout le monde sans exception, qui a favorisé les erreurs informatiques et technologiques graves et dont profitent pleinement les cybercriminels.

Section 1 : L'évolution des risques cybernétiques dans le monde

1. Définition et exemples :

La gestion des risques est un acte d'équilibre pour les organisations de différentes tailles et disciplines. Et suite à cette diversité, certaines organisations prennent trop de risques alors que d'autres ne prennent pas assez. Ce qui rend plus compliquée la situation, et notamment l'émergence du cybernétique comme l'une des sources de risque les plus percutantes caractérisant l'entreprise moderne. En fait, la Cybersécurité est maintenant de plus en plus examinée par les conseils d'administration des entreprises et souvent discutée avec les analystes financiers qui considèrent le risque cybernétique comme un risque opérationnel imminent et prépondérant. En effet, les conséquences des attaques cybernétiques peuvent nuire aux revenus de l'entreprise et à sa réputation.

La mondialisation, les fusions et les acquisitions, l'extension des réseaux et des relations avec des tiers, l'externalisation, l'adoption de nouvelles technologies, le mouvement vers le Cloud, et la mobilité sont toutes des sources de risques cybernétiques et cette démarche de modernisation ne va jamais s'arrêter. Le risque cybernétique est né de l'intersection du risque de la commercialisation, de la réglementation et de la technologie. Les décideurs exécutifs doivent, donc, comprendre la nature et l'ampleur de ces risques et prendre toutes les mesures possibles pour y faire face[1].

Le risque cybernétique est généralement défini comme l'exposition aux dommages ou aux pertes résultant de violations ou d'attaques contre les systèmes d'information. Ces attaques peuvent être catégorisées de plusieurs façons. La plus répandue est l'intention c'est-à-dire que

1

CYBER RISK APPETITE:
Defining and Understanding Risk in the Modern Enterprise

les faits soient intentionnels ou non. Les événements peuvent être le résultat d'actes malveillants, tels qu'un piratage dans le but de compromettre des informations sensibles, comme ils peuvent, également, être involontaires, comme une erreur lors de l'utilisation ou de la manipulation d'un système le rendant temporairement indisponible.

Les risques cybernétiques peuvent 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 (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.

La fréquence et la gravité des bris de sécurité, des pannes de système et des vols de données augmentent à un rythme alarmant partout dans le monde. Si un secteur d'activité recueille, stocke et utilise des données financières ou médicales sur des individus, tel est le cas des institutions financières, des établissements d'enseignement, des commerces de détail, des sociétés de télécommunications, des entreprises de services publics, des municipalités, des

compagnies d'assurance ou des associations médicales, alors ce secteur est particulièrement à risque en matière de vol d'identité et d'informations confidentielles. La cybercriminalité est considérée comme un leader incontesté dans le monde des risques vu sa capacité de toucher à la fois des centaines de millions de victimes. En effet, Une estimation a montré que les deux tiers des personnes en ligne, c'est-à-dire plus de deux milliards d'individus, ont eu leur propre information volée ou mise en péril[2]. C'est un crime à faible risque pour les hackers et qui procure des gains élevés. Un cybercriminel futé peut faire des centaines de milliers, même des millions de dollars avec presque aucune chance d'arrestation quand on se rappelle des grands crimes cybernétiques, telles qu'exposées dans ce tableau :

Tableau 1: Les plus grands crimes cybernétiques dans le monde

Année	Victime	Pertes	Hacker
2010	Paypal	$4 millions	Anonymous
2011	Le gouvernement Tunisien	Piratage des sites et portails internet clés du gouvernement tunisien.	Anonymous
2012	Fbi.gov	$2.5 million	Anonymous
2013	Corée de Sud	$650 million	Inconnu
2014	Sony Pictures	$30 million	Inconnu
2015	ANTHEM Health Insurance	Les données de 80 millions clients	Inconnu
2016	Yahoo	500 million comptes piratés	Inconnu
2017	Uber	$ 81000	Inconnu
2018	Porsche Japan	24 000 adresses mail piratées	Inconnu

Source : Journal New York Times

On peut constater que la plupart des criminels cybernétiques restent inconnus auprès des autorités et même si un groupe de hackers déclare son crime il est rarement poursuivi vu que, généralement, ces groupes sont composés de plusieurs membres et que leurs identités sont difficilement reconnaissables.

2. L'évolution des risques cybernétiques dans le monde :

2.1.Par région

[2] "Americans and Cybersecurity" Pew Research Center, January 26, 2017).

La figure 1 représente le coût estimé des crimes cybernétiques en millions de dollars pour sept pays différents, l'étude est faite sur un échantillon de 254 compagnies d'activités différentes entre les années 2016 et 2017.

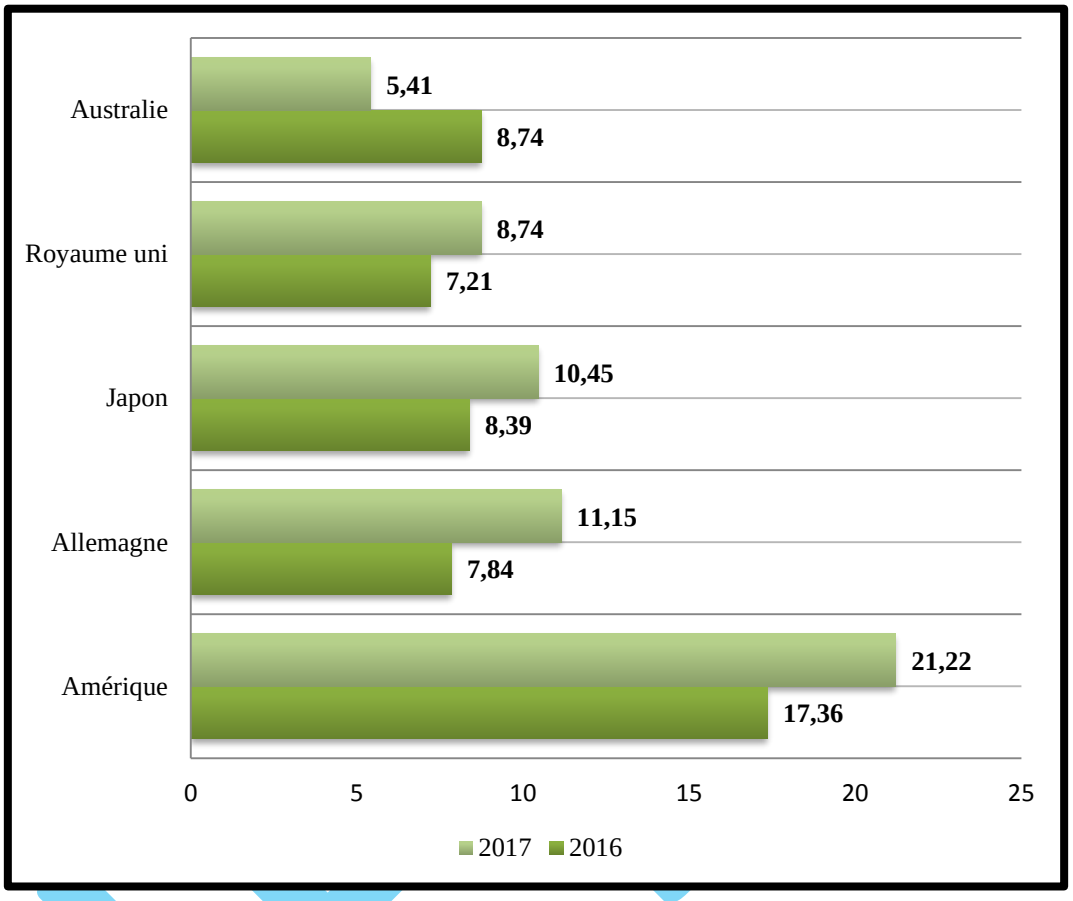


Figure 1: Evolution du coût des attaques cybernétiques en millions de dollars entre 2016 et 2017

Source : www.statista.com

Les compagnies en Amérique présentent le coût le plus élevé avec une évolution de **22,2%**, pendant que l'Australie présente le cout le plus faible avec une évolution négative de **25,8%**. Le pays qui présente l'évolution la plus élevée est l'Allemagne avec **42,4 %** tandis que le Royaume uni présente la plus faible avec **21%**.

2.2.Par secteur d'activité :

La figure 2 représente le coût annuel moyen des incidents cybernétiques par secteur d'activité dans le monde en 2017, la classification est basée selon 15 secteurs différents. Comme le montre la figure ci-dessous, le coût annuel moyen des crimes cybernétiques est le plus élevé pour le secteur financier et énergétique tandis que les compagnies d'éducation et le secteur hôtelier représentent le coût le plus faible.

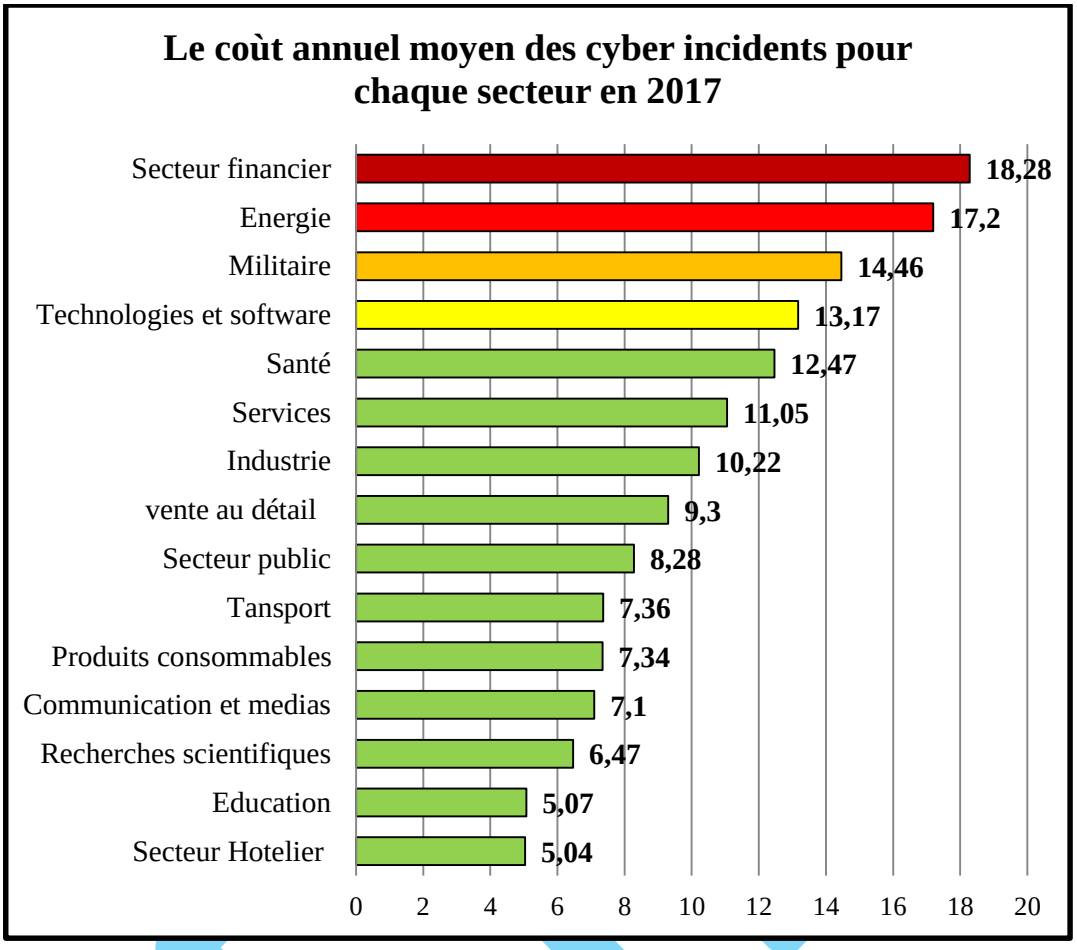


Figure 2: Le coût annuel moyen des incidents cybernétiques par secteur

Source : 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 million** et de **$2 million** 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 (Botnet est un terme générique qui désigne un groupe d'ordinateurs infectés et contrôlés par un pirate à distance) pour des coûts respectifs de **$532,914** et **$350,012 milles**.

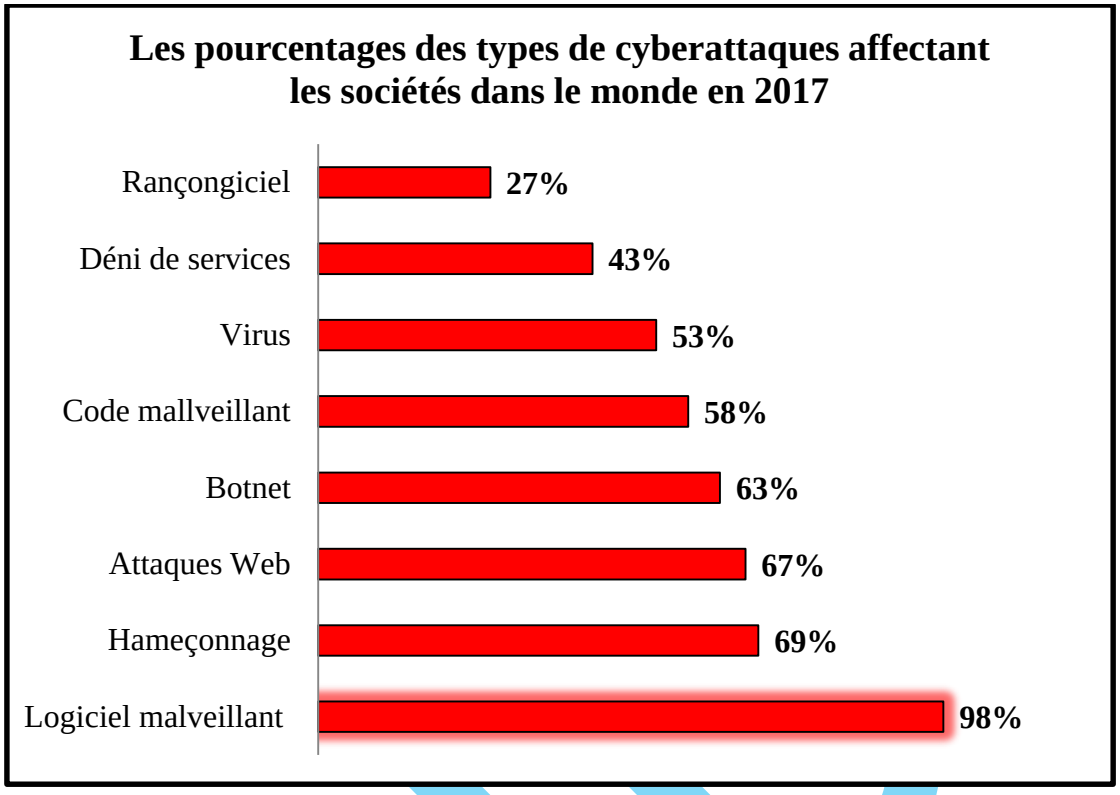


Figure 3:Le pourcentage de chaque type d'attaque cybernétique dans le monde pour un échantillon de 254 sociétés

Source : www.statista.com

Le graphique ci-dessus résume une étude faite sur 254 sociétés dans le monde qui ont été victimes d'un cyber incident en 2017, nous pouvons constater que **98%** des compagnies ont été affecté par un logiciel malveillant ,**69%** par un hameçonnage tandis que **27%** seulement ont été affectées par un Rançongiciel.

3. Les moyens de prévention :

Les moyens de prévention contre les attaques cyber sont multiples, elles peuvent atténuer le risque mais elles ne peuvent jamais l'annuler ou l'empêcher, le risque zéro en informatique est inexistant[3].

En observant la figure 4 ci-dessous, on peut constater que le moyen de sécurité qui peut économiser le plus en matière de risques cyber est offert par les systèmes de renseignement de sécurité avec une économie de presque **$3millions** alors que l'économie la plus faible est fournie par la gestion automatique des fichiers qui permet uniquement une économie de **$590000**.

[3] La cybercriminalité au Maroc, 2010

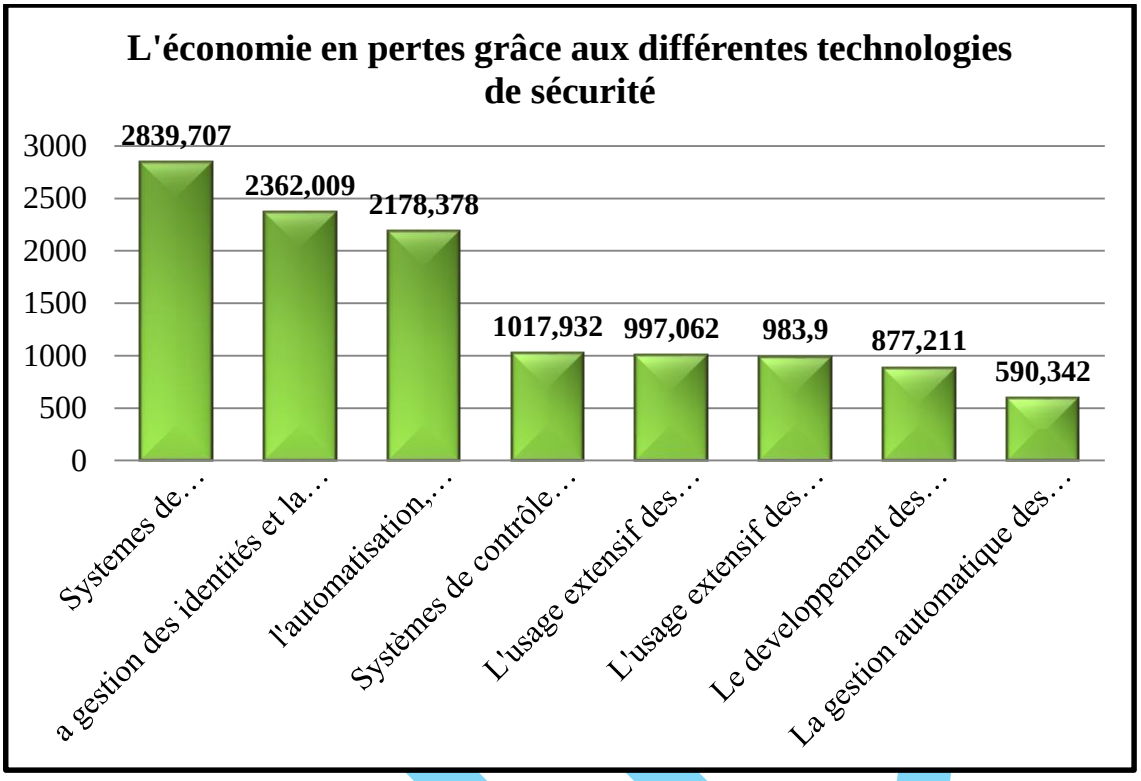


Figure 4: L'économie en pertes grâce aux différentes technologies de sécurité

Source : www.statista.com

4. Le rôle de l'assurance des risques cybernétiques dans le monde :

Les conséquences d'un cyber incident sont l'une des conduites les plus méprisables qu'un humain peut imaginer. Malheureusement, les nouvelles technologies liées à la digitalisation ont permis l'aggravation de ce phénomène et ont rendu la tâche lourde pour les moyens de cybersécurité.

Pour comprendre davantage la cybersécurité, il est primordial de décortiquer la notion de la sécurité de l'information vu que ce fait tient son extension à l'insécurité liée l'utilisation des nouvelles technologies d'information. Or, souvent on comprend mal le concept de sécurité. D'où le besoin nécessitant de jeter un coup d'œil sur cette notion dans le but de mieux en comprendre les enjeux.

Pour la majorité des organisations, sécuriser son système d'information est limité à la dimension technologique, c'est à dire la mise en place d'un antivirus et d'un pare feu. Cependant, ces mesures ne sont pas suffisamment utiles lorsqu' il s'agit, par exemple, d'une attaque Dos (Denial of Service (DoS) : Dénis de Service en français, c'est une attaque qui a

pour but de rendre indisponible, totalement ou partiellement, un système informatique), qui évolue ces dernières années d'une manière spectaculaire[4].

La sécurité est un concept tridimensionnel, donc on ne peut pas parler uniquement de la dimension technologique et négliger les dimensions organisationnelle et humaine surtout quand on se rappelle des organisations comme le FBI ou le Pentagone qui ont été victimes d'attaques cybernétiques importantes qui, certainement, ne manquent pas de dispositifs de protection techniques sophistiqués ce qui nous conduit au fait que la faille est plutôt organisationnelle voir humaine.

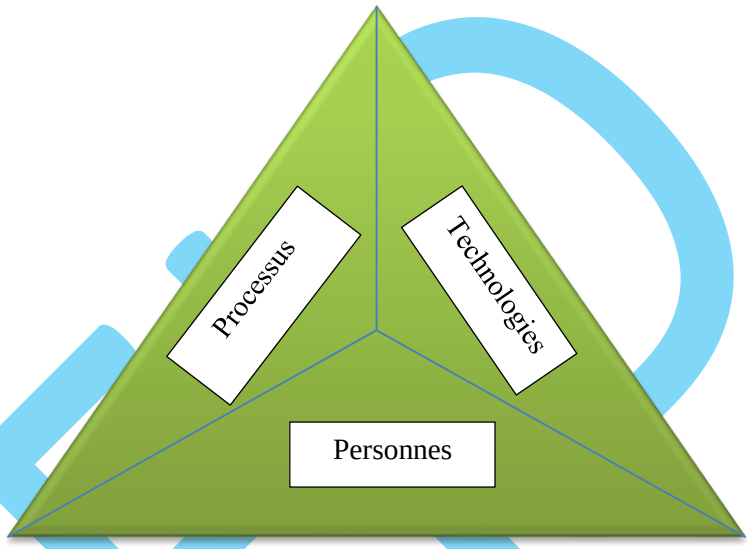


Figure 5: Les trois dimensions de la sécurité

Source : la cybercriminalité au Maroc

Certainement, l'investissement dans la mise en place des moyens techniques préventifs, défectifs et correctifs des problèmes de sécurité est inévitable. En contrepartie, le volet organisationnel consistant à l'instauration d'une politique veillant à la sécurité de l'information, à la mise en place d'une charte organisant l'utilisation des ressources ainsi qu'une multitude de procédures et processus opérationnels afin d'assurer un niveau minimal de sécurité est aussi vital pour l'organisation. En effet, nous constatons souvent, que la dimension technologique est moyennement maîtrisée. La nature des failles identifiées est généralement organisationnelle.

Il faut aussi prendre au sérieux la dimension humaine qui est à l'origine de plusieurs attaques lorsque, par exemple, le personnel d'une organisation n'est pas suffisamment formé ou

[4] 2017 cyber claims study

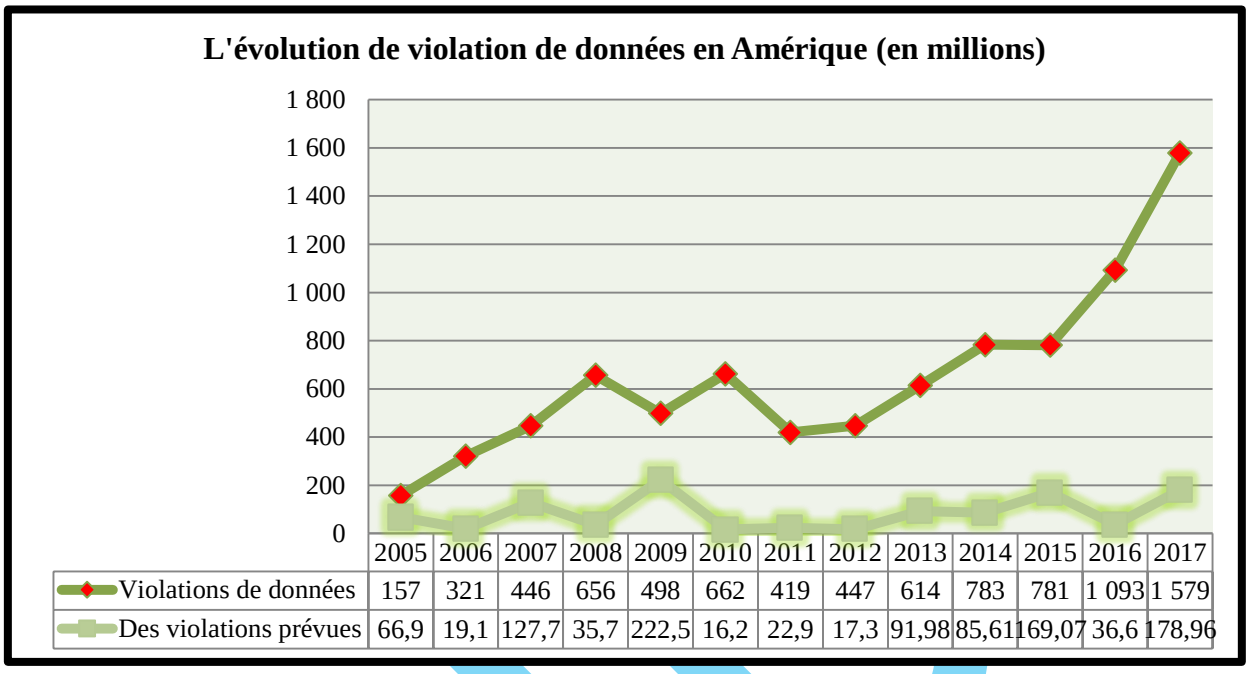
sensibilisé, aucune mesure de sécurité sur le plan organisationnel ou technologique ne serait efficace face aux attaques et incidents cybernétiques éventuelles.

L'être humain est qualifié de maillon faible de la chaine de sécurité. Les pirates ont identifié cette faille et ont orienté leurs efforts vers cette perspective pour récupérer plus d'informations.

On peut dire donc que la sécurité cybernétique plus particulièrement celle des données et informations confidentielles constitue l'un des premiers soucis lorsqu'on parle de risques des entreprises. Plusieurs organisations confirment que les systèmes de sécurité, même les plus sophistiqués, ne sont pas infaillibles. Cela conduit les entreprises à s'orienter vers un moyen plus sûr qui est notamment la souscription des polices d'assurance cyber offrant une panoplie de couvertures en face d'un éventuel sinistre résultant d'un risque cybernétique.

Le marché Américain est le plus grand marché à l'échelle internationale avec **$2.7bn** l'équivalent de **90%** de primes d'assurance des risques cybernétiques en 2015. C'est l'acteur principal dans l'évolution des primes en assurance cybernétique. Cette évolution impressionnante est due à plusieurs facteurs. Les lois et les régulations veillant à la protection des personnes et des organisations contre la violation des données est particulièrement accrue en Amérique. En outre, 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. On peut citer quatre facteurs principaux qui ont fait du marché Américain un leader dans la matière :

Le coût annuel moyen d'une violation de données coûte en moyen aux États-Unis entre **$ 1.1 millions** et **$ 3.8 millions** en 2017 avec une évolution surprenante.



	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Violations de données	157	321	446	656	498	662	419	447	614	783	781	1 093	1 579
Des violations prévues	66,9	19,1	127,7	35,7	222,5	16,2	22,9	17,3	91,98	85,61	169,07	36,6	178,96

Figure 6: L'évolution de violation de données en Amérique en millions entre 2005 et 2017

Source : www.statista.com

Le graphe ci-dessus présente le nombre enregistré de violations de données et d'enregistrements exposés aux États-Unis entre 2005 et 2017. Au cours de la dernière année le nombre de violations de données aux États-Unis s'élevait à **1 579** millions avec près de **179 millions** de violations prévues.

Les violations de données ont attiré l'attention avec l'utilisation croissante de fichiers numériques que les entreprises et les utilisateurs particuliers les utilisent largement. Même si les violations de données se produisaient avant la numérisation de l'information - par exemple, l'examen de documents médicaux sans autorisation peut être considéré comme une violation de données, la popularité des plates-formes numériques a porté une nouvelle dimension au volume et à l'importance des données. Les données exposées ont, donc, considérablement augmenté et devenues de plus en plus à la portée de tous. Dans le monde entier, le vol d'identité est le type d'incident de violation de données le plus courant, représentant **59%** de tous les incidents de violation de données en 2016.

On peut voir parallèlement, dans le graphe ci-dessous, l'évolution des primes d'assurance cybernétique dans le monde.

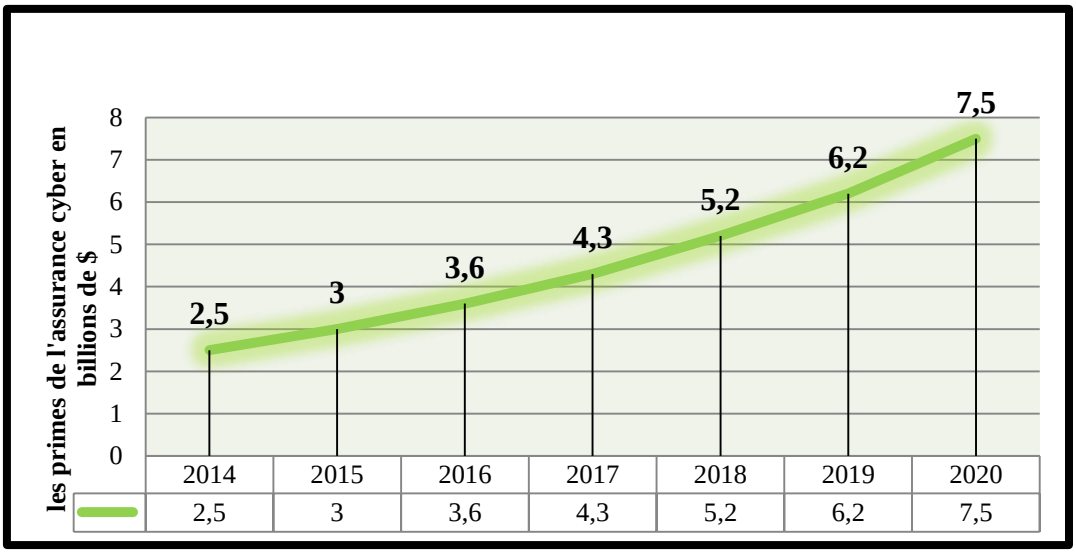


Figure 7: L'évolution des primes d'assurance cyber dans le monde de 2014 à 2020

Source : www.statista.com

Une évolution qualifiée d'exponentielle avec un volume de primes qui atteint **$4,3bn** en 2017 et qui est estimée atteindre **$ 7,5bn** en 2020.

La figure suivante peut mettre en valeur l'évolution et l'aggravation des risques cybernétiques durant la dernière décennie, en effet, le graphe montre le nombre de vulnérabilités c'est-à-dire les failles dans les systèmes de sécurité informatique qui peuvent conduire à des incidents cyber dans le monde entre **2009** et **2017**. Par exemple, la dernière année présente **14712** nouvelles vulnérabilités c'est-à-dire le **double** du nombre repéré l'année d'avant.

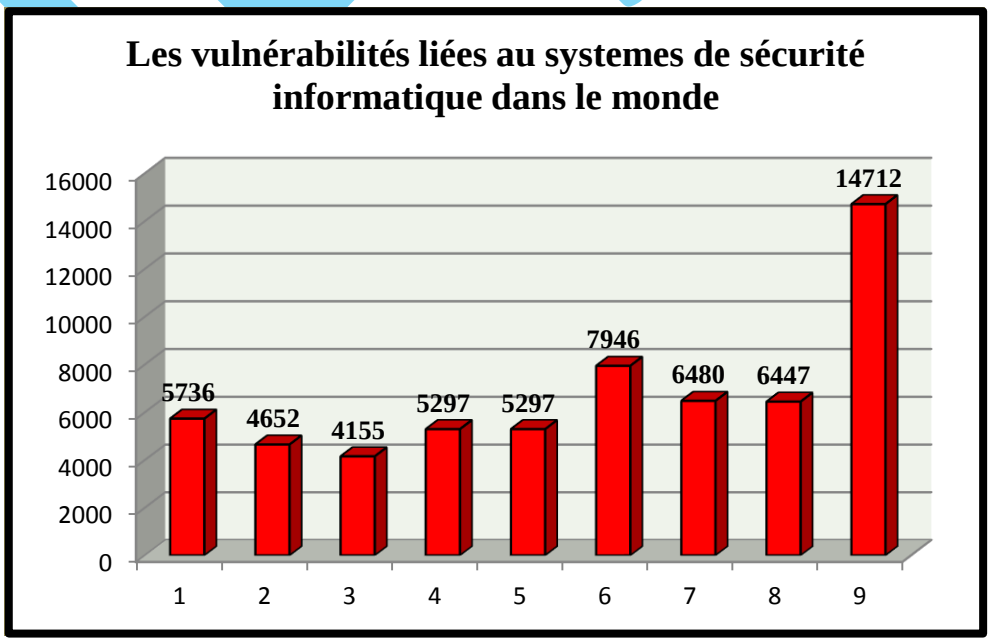


Figure 8: Les vulnérabilités aux risques cyber dans le monde

Source : www.statista.com

Une attaque cybernétique peut causer plusieurs dégâts qu'on peut classifier sous quatre grandes catégories :

- Perte d'information
- Interruption des affaires
- Perte de revenu
- Matériel endommagé

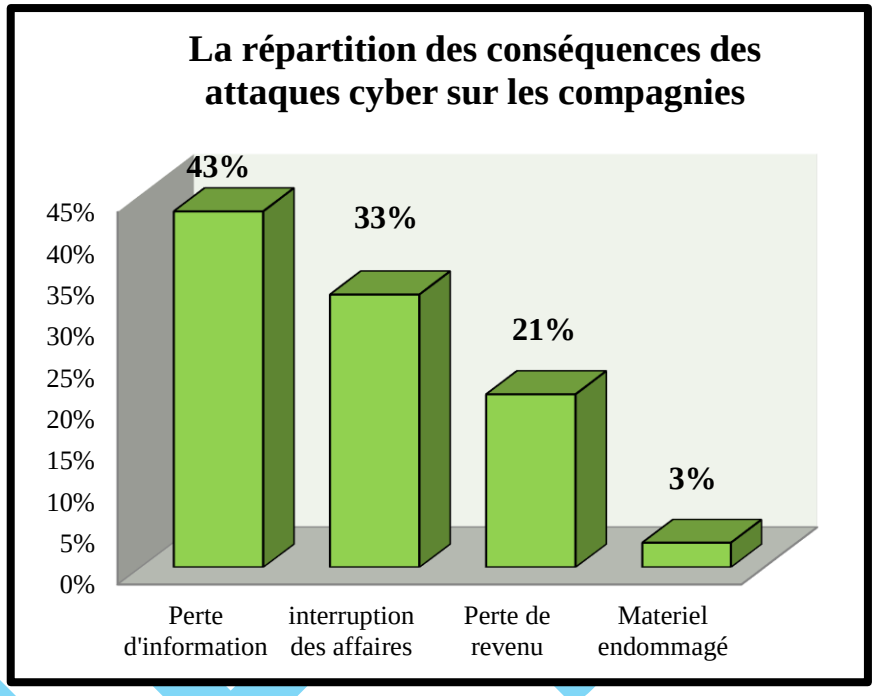


Figure 9: Les pourcentages des conséquences des attaques cyber sur les compagnies dans le monde

Source : www.statista.com

Les statistiques ci-dessus fournissent des informations sur la répartition des coûts des conséquences externes des cyberattaques ciblées sur les entreprises dans le monde en 2017. On remarque que **43%** des coûts d'une cyberattaque ciblée sont liées à la perte de données alors que **3%** seulement résulte du matériel endommagé suite à une attaque cyber.

Pour mieux comprendre l'importance et la nécessité de la souscription d'une police d'assurance cybernétique, on a cité dans le tableau suivant une liste des cas concrets qui ont été victimes de cyberattaques et dont la majorité a bénéficié d'une indemnité. Les sociétés citées ci-dessous sont toutes des références dans le monde des affaires et elles sont dotées de systèmes de sécurité sophistiqués.

Tableau 2: Exemples de cyber attaques assurés

Victime	Cause	Coût total	Coût assuré
Epsilon	Hameçonnage ciblé	Jusqu'à 4 milliards de dollars	Aucune protection en place
Home Depot	Défaillance du système de cyber sécurité du fournisseur et du système de sécurité de Microsoft Windows	$ 232 millions	100 millions $
Administration des anciens combattants	Ordinateurs/Disques durs externes soi-disant volés à la maison de l'employé lors d'un vol avec effraction	500 millions $	Aucune protection en place
Target	Défaillance du système de cyber sécurité du fournisseur	252 millions $	90 millions $
Hannaford Bros.	Logiciel malveillant	252 millions $9; responsabilité de l'assurance pour vol d'identité et coût de la carte de remplacement10	Aucune protection en place
Sony PlayStation	Inconnue	171 millions $	Inconnu; règlement dans l'attente de l'appel après que la cour ait rendu un jugement sommaire à l'encontre de Sony12
TJ Maxx	Réseau local sans fil mal sécurisé dans deux magasins13	256 millions $	19 millions $
Sony Pictures Entertainment	Corée du Nord	151 millions $ + atteinte à la réputation	151 millions $
Heartland Payment Systems	Attaque DDoS	140 millions $	30 millions $

Source : La cybersécurité : l'incidence sur le domaine et les opérations de l'assurance

5. L’assurance cyber et les banques

Classés parmi les risques majeurs, les cyberrisques sont encore méconnus et leurs conséquences sont, souvent, sous évalués par les décideurs dans les entreprises. Le risque informatique représente la menace la plus importante pour le système financier mondial, en effet, les données constituent le patrimoine des entreprises du secteur bancaire et financier. La montée en puissance du **big data**, des **fintech** ou encore du **blockChain** font d’elles une cible privilégiée des cybercriminels. La figure suivante, publiée par la fédération française de l’assurance, montre que le risque technologique est le risque le plus important au niveau du secteur financier et qu’il le restera jusqu’au 2022.

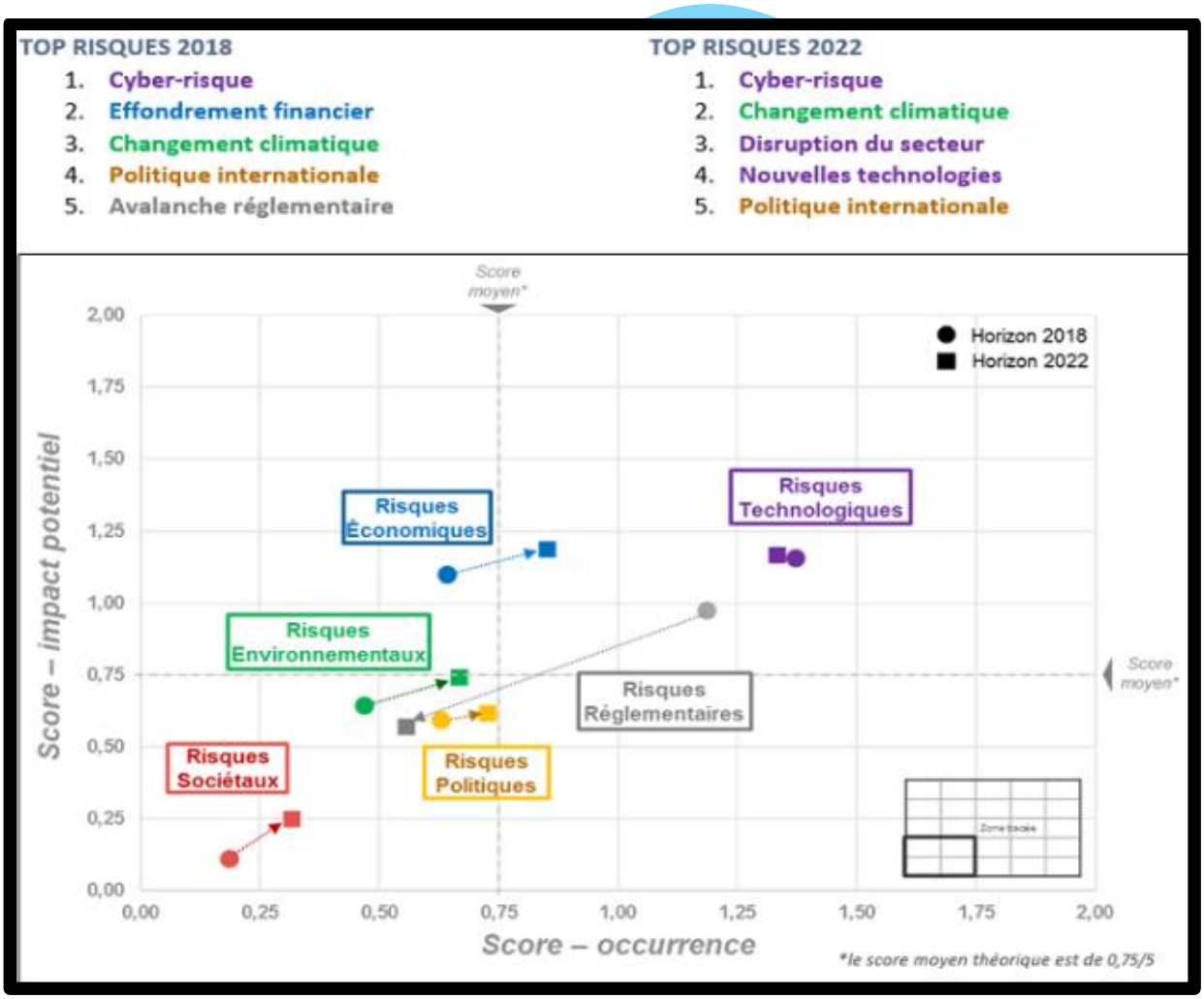


Figure 10: Les top risques émergents

Les directions générales sont de plus en plus sensibilisées à ce risque systémique : appréhender, mesurer les risques cyber, se protéger, sécuriser ses données et ses systèmes d’information est devenu l‘enjeu du secteur bancaire et financier.

De nombreuses entreprises ne se sont pas encore assurées parce que leurs dirigeants ne font pas souvent le lien entre protection des données et assurances. Rare est ,d’ailleurs, le

consultant en cybersécurité en charge de l'audit des systèmes d'information qui va s'associer à une compagnie d'assurance pour offrir un système d'information entièrement sécurisé ainsi qu'une couverture des risques appropriée. Il y'a huit raisons, d'après Lloyds Bank, qui justifient la nécessité de la souscription d'une assurance cyber [5]:

*Protéger sa réputation

*Les données sont le patrimoine de la banque

*La responsabilité à l'égard d'une tierce partie de toute donnée perdue

*Les crimes cybernétiques évoluent d'une manière exponentielle

*Le dysfonctionnement d'un système peut causer une perte énorme suite à l'interruption de l'activité ainsi que les frais de réparation

*Les appareils portables qu'on utilise quotidiennement tels que les ordinateurs et les téléphones constituent une menace.

*Les réseaux sociaux sont un outil puissant mais il peut nuire à la confidentialité des informations ainsi que la réputation de la société.

* Même les petites entreprises peuvent être une cible pour les cybercriminels.

Parfois la grande menace, et souvent l'une des plus difficiles à détecter, est celle des utilisateurs malveillants, négligents et compromis. Ces employés, sous-traitants et partenaires sont déjà à l'intérieur du périmètre sécurisé de la banque et ont un accès légitime à ses données sensibles et à ses systèmes informatiques. Lorsque ces initiés abusent de leur accès privilégié ou sont compromis par des attaquants externes, les données précieuses sont facilement divulguées. En outre, comme les banques continuent d'étendre l'accès en ligne et mobile, elles étendent également la surface d'attaque. En tant que tels, ils doivent être vigilants contre les attaques DDoS et les attaques d'applications Web.

Au cours de la dernière décennie, nous pouvons voir de nombreuses violations très médiatisées contre de grandes institutions de services financiers, et le volume et la complexité des attaques sont en hausse.

Les criminels peuvent envoyer des courriels d'hameçonnage ou créer de faux sites Web qui trompent les consommateurs en leur permettant de divulguer des données financières sensibles. Ils peuvent également exploiter les informations réseaux sociaux pour s'introduire dans les comptes des clients.

[5] www.lloydsbank.com

Section 2 : Aperçu sur le marché national

La Tunisie présente 11 millions 450 mille habitants dont **68%** sont des utilisateurs actifs d'internet soit donc 7.89 Million habitants, et **60%** sont des utilisateurs d'internet mobile (à travers les Smartphones) soit 7.01 Million habitants. Des pourcentages importants, certes, dans un cadre qui n'est pas parfaitement sécurisé là où la fraude peut se commettre aisément sans laisser aucune trace. [6]

Aujourd'hui, la Tunisie se prépare pour une révolution digitale avec le e-Gouvernement, le e-Banking, le e-commerce et pourquoi pas le e-Insurance là où le risque cyber est omniprésent, de ce fait elle doit faire face à tous les incidents qui peuvent accompagner cette vague de modernisation.

1. La Tunisie et la digitalisation :

Nous assistons depuis plus de trente ans à une forte incitation des économies les plus avancées à la création d'entreprise et l'émergence croissante de start-ups dans l'économie numérique ou dans les industries créatives. Ainsi, la mise en place d'un système économique favorable à leur expansion est devenue un impératif de compétitivité économique. La transformation digitale est en train de toucher l'économie dans son ensemble, des nouvelles politiques industrielles sont mises en place dans plusieurs pays.

Des secteurs entiers de l'économie subissent une transformation profonde, des filières disparaissent et d'autres vont suivre, alors que de nouvelles émergent. La majorité des métiers se transforment, plus de 60% des métiers de demain ne sont pas encore définis aujourd'hui.

Le programme « Smart Tunisia », est une composante fondamentale de la stratégie nationale " Tunisie Digitale 2020 " a conclu sept conventions, de partenariat, avec des organisations et des associations actives dans le domaine de la technologie et du numérique, afin de créer trois milles emplois pour les diplômés de l'enseignement supérieur. Durant le dernier quinquennat, Le positionnement de la Tunisie, à l'international, a été rétrogradé[7] :

L'indice : « Networked-Readiness-Index » (NRI) du Forum Économique Mondial : la Tunisie passes du 50ème rang en 2012, au 87ème en 2014 et au 81ème en 2015. La Tunisie est classée 4ème en Afrique et 8ème dans le monde Arabe.

L'indice « UN-Global-E-Government-readiness-survey » évaluant le niveau d'application des technologies de l'information et de la communication (TIC) : La Tunisie était classée, en

[6] 2018 Digital yearbook
[7] www.jeuneafrique.com

2010, 66ème, puis en 2012, 103ème puis elle reprend, en 2015, la 72ème position de sur 192 pays.

L'indice « AT-Kearney-Global-Service-Location-Index » qui a pour but d'évaluer la qualité des destinations d'outsourcing : Donne une rétrogradation de la Tunisie de la 17ème classe en 2010 et à la 38ème position en 2016.

Pour conclure, la numérisation et malgré sa croissance spectaculaire durant la dernière décennie, n'arrive pas à, réellement, stimuler l'économie de la Tunisie qui présente des performances, presque, stagnantes ou, voir, rétrogradées ces dernières années.

Pour remédier à ça, le plan national stratégique « PNS Tunisie Digitale, 2018 » conçu en 2014 en coopération avec toutes les parties prenantes, a pour ambition d'être une référence internationale dans le domaine du numérique et de compter sur les technologies de l'information et de la communication les plus sophistiquées pour réaliser une croissance sur le plan économique et social.

Ce PNS envisage, donc, de :

- ✓ Faire participer toute la population et les entreprises dans le sphère de l'économie numérique
- ✓ Réaliser l'équité sociale à travers un accès au savoir pour tous les individus
- ✓ La stimulation du système économique, de l'innovation et de la créativité.
- ✓ Implanter le concept « Administration sans papier »

Généraliser l'usage de nouvelles technologies dans la stratégie pédagogique

2. L'évolution des risques cybernétiques en Tunisie :

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. Dans le graphe suivant on peut voir l'évolution des vulnérabilités en Tunisie. Dans le domaine de la sécurité informatique, **une vulnérabilité ou faille est une faiblesse dans un système informatique 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.

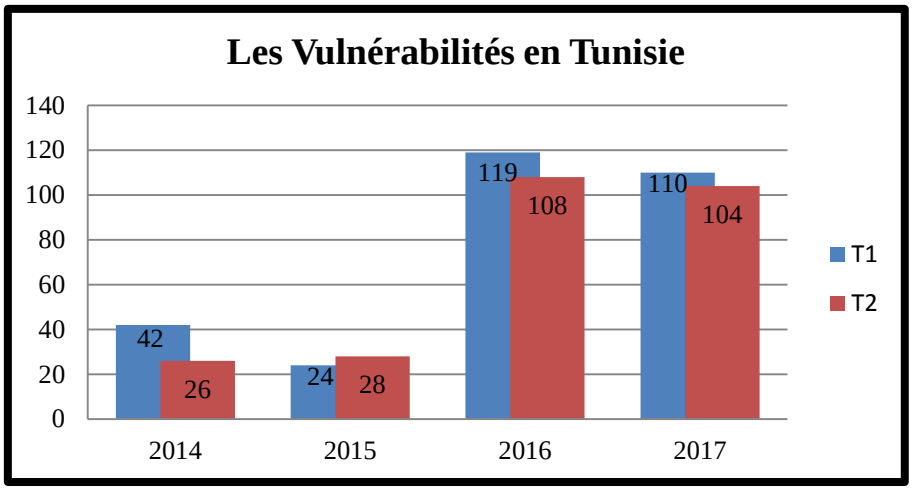


Figure 11: Les vulnérabilités en Tunisie

Source : www.statista.com

On peut remarquer que les vulnérabilités ont évolué exponentiellement les deux dernières années pour atteindre **110** et **104** les deux premiers trimestres de 2017 comparé à **24** et **28** en 2015. Dans le monde, la Tunisie est classée **deuxième** en terme des internautes les plus affectés par les attaques cyber en 2014 après Kenya comme le montre ce graphe :

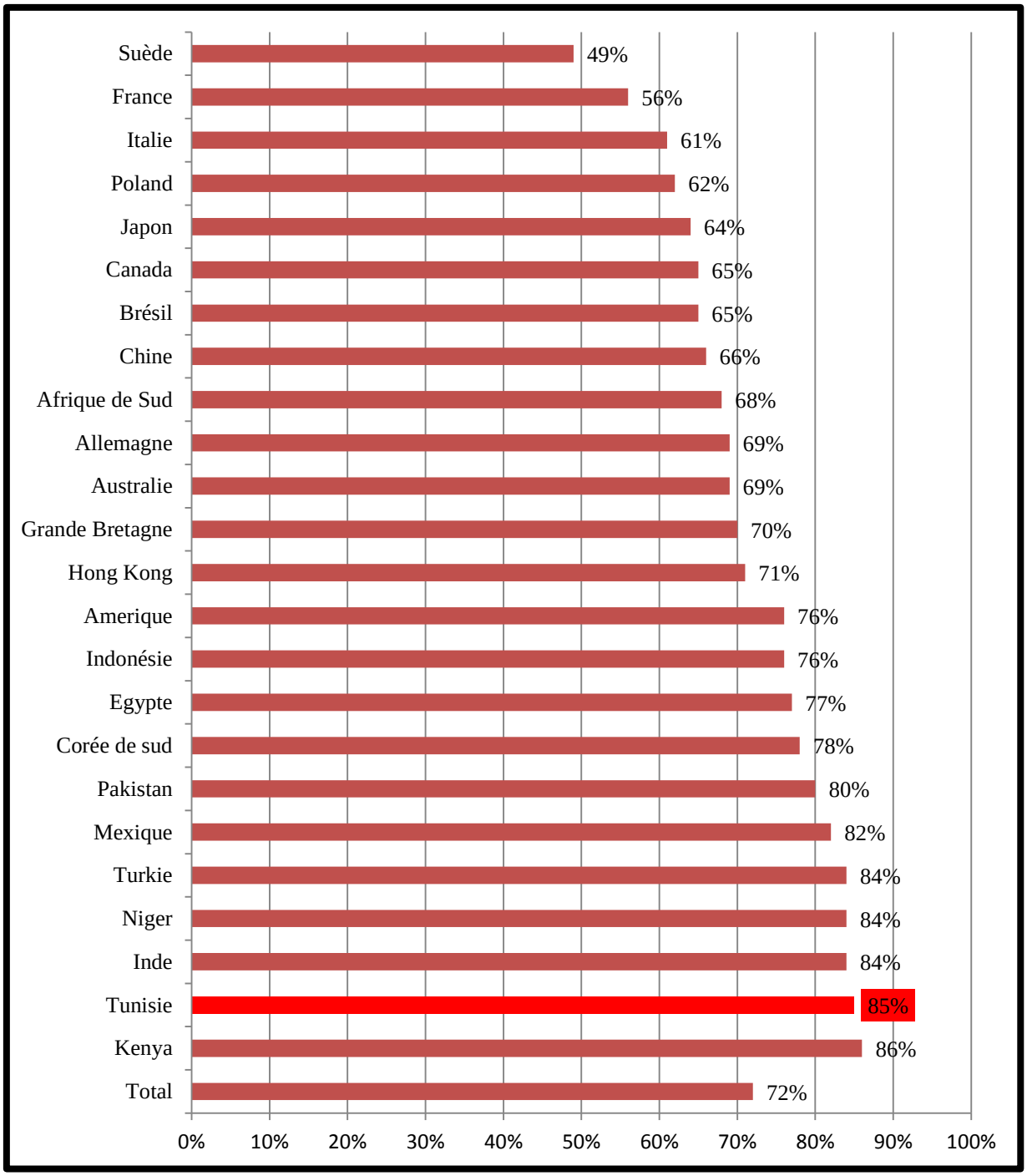


Figure 12: Le classement de la Tunisie dans le monde en terme des internautes les plus affectés par les attaques cyber en 2014

Source : www.statista.com

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 le graphe suivant, on peut voir que la Tunisie occupe la 6ème place dans le classement des banques les plus affectées par les logiciels malveillants dans le monde avec **2,21%** de la totalité des attaques.

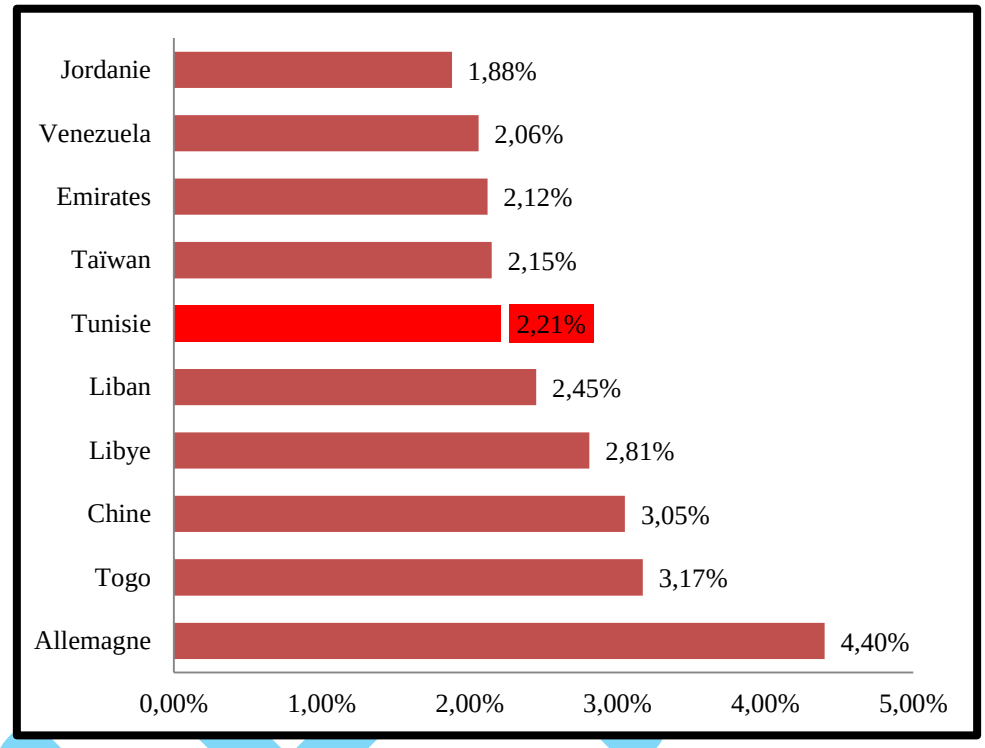


Figure 13:Les banques les plus affectées par les logiciels malveillants dans le monde

Source : www.statista.com

Il y'a plusieurs types d'attaques qu'on peut classifier de la sorte :

- Le drive-by (il s'agit d'un code malveillant introduit pour détecter une défaillance au niveau de la sécurité d'un réseau web)
- La diffusion de virus, chevaux de Troie, et logiciels espions (spywares) ;
- Les botnets (réseau de machines zombies infectées par des virus et corrompues par des programmes malveillants)
- Le DDoS (Distributed Denial of Services) ou attaque par déni de services distribués ;
- La diffusion de spam et pollupostage (envoi de courriers électroniques indésirables à un grand nombre de destinataires)
- Les différentes formes d'hameçonnage et de cyber-escroquerie par voie de courriels
- La violation de données et usurpation d'identités en ligne
- La diffusion de Scareware (logiciels de sécurité non autorisés et illégaux).

Les types d'attaques en Tunisie sont à répartir de la sorte :

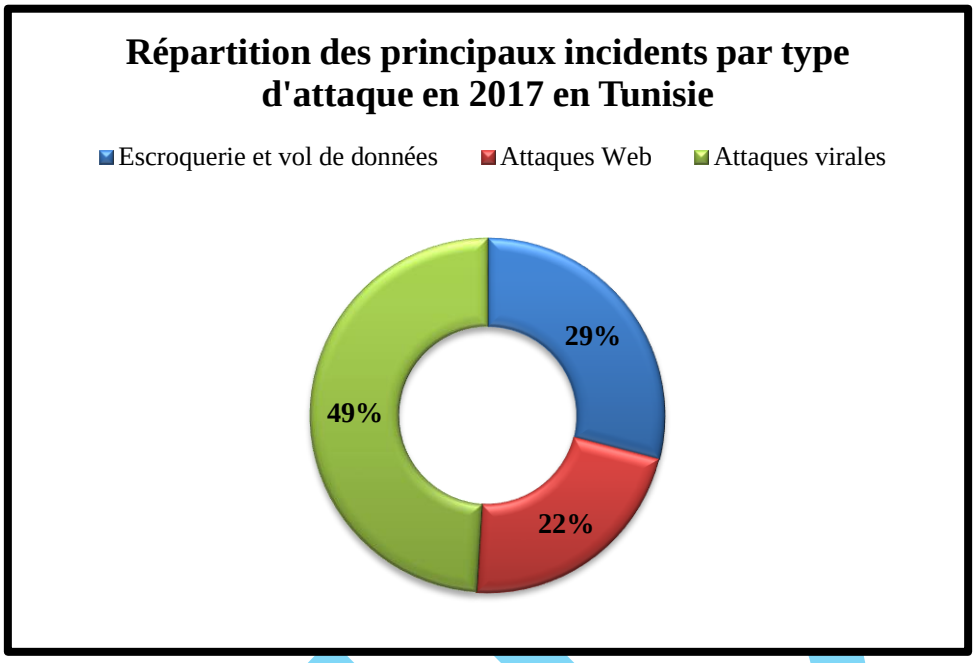


Figure 14: Répartition des principaux incidents par type d'attaque en Tunisie en 2017

Source : Agence Nationale de Sécurité Informatique

3. La Tunisie et le cyber Terrorisme :

Ces dernières années, la Tunisie a réussi à abattre, neutraliser de nombreuses cellules terroristes et à freiner de nombreux projets de subversion en coopération avec des partenaires internationaux. A cet égard, la Tunisie veille à mettre en œuvre des mécanismes juridiques pour lutter efficacement contre le Cyberterrorisme[8].

Prenant en considération tous les efforts fournis pour gouverner le domaine de l'information et de la communication, quelques lacunes majeures visant à prévenir les actes de Cyberterrorisme et à protéger les citoyens et les droits de l'homme persistent encore, y compris celles notées ici:

- 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.
- Dans le contexte d'un gouvernement ouvert c'est-à-dire régi par une doctrine de gouvernance qui vise à améliorer l'efficacité et la responsabilité des modes de gouvernance publique, il est impératif d'ajuster la classification des données sensibles, telles que celles

[8] Tunisian national risk assessment of money laundering and terrorist financing

liées aux informations critiques et sélectionner avec trop de prudence les informations qui peuvent être publiés sans qu'elles soient exploitées par les cyber-terroristes.

- En outre, l'absence d'un cadre réglementaire qui permet l'utilisation des réseaux sociaux par les citoyens et les organismes gouvernementaux pour suivre et surveiller les cyber-terroristes.

Et ce manque de règlementation peut être justifié par le fait que toute réglementation peut constituer une limite de la liberté de l'utilisation d'internet qui va l'encontre de la liberté d'expression , d'information et de la confidentialité et la protection des données.

Pour faire face aux effets néfastes du cyber terrorisme sur l'économie, l'infrastructure ainsi que sur le plan social et psychologique il faut mettre en place une approche stratégique qui porte principalement sur quatre axes :

Le cadre législatif :

-Adopter une réglementation qui gère le monde virtuel en rapport avec les diverses menaces posées par le Cyberterrorisme y compris le suivi des plateformes des réseaux sociaux afin de détecter, répondre et dissuader toute propagation possible de la propagande terroriste, la communication de la radicalisation entre les individus et les éléments terroristes connus, les activités d'extraction de données dans le but de planifier des attaques terroristes ou le recrutement de personnes et d'autres Internet liés au terrorisme coutumes; ainsi que le suivi des activités terroristes dans le « Dark Net ». Des mécanismes adéquats assurant le respect de la liberté d'expression et la vie privée doit être développée. De plus, le suivi devrait être effectué avec cohérence et l'intégrité pour cibler les terroristes et d'autres 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 gens et les autorités aussi par la menace que présente l'univers cyber pour la société.

Une stratégie nationale :

Une stratégie de gestion des risques pour identifier et caractériser les menaces cyber, savoir évaluer la vulnérabilité des actifs critiques à ces menaces, déterminer le risque et se procéder rapidement à réduire ces risques avant que la vulnérabilité ne se transforme en une attaque effective.

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 prévention et les bonnes pratiques :

Dans ce contexte bien précis et face aux risques cyber, il est recommandé d'identifier les systèmes sensibles et surtout ceux qui sont exposés sur Internet et de vérifier l'application des règles de sécurité conformément à la politique de sécurité interne :

- S'assurer de la sécurité au niveau de la plateforme d'hébergement.
- Vérifier le déploiement des solutions de sécurité nécessaires: contrôle antiviral, filtrage, détection d'intrusion et filtrage applicatif.
- S'assurer de l'utilisation des dernières versions des systèmes de gestion
- Auditer votre application web pour identifier les failles qui peuvent être exploitées, en faisant appel à un expert dans le domaine si c'est possible.
- Appliquer les bonnes règles de gestion : Contrôle d'accès à la zone d'administration, gestion de mots de passe, vérification du login, sauvegarde des données, plan de secours en cas de problème majeur, utilisation des protocoles sécurisés pour l'administration à distance tels que : HTTPS, SSH, SCP.
- Avoir une procédure de veille pour s'informer sur les nouvelles failles et appliquer les correctifs en un temps optimal.
- Vérifier la sécurité de votre poste d'administration.

En cas de cyber-attaque et/ou d'une violation de données, l'entreprise doit faire face à une cyber-crise dont la multiplicité des conséquences (juridique, financière et réputationelle) peut être irrémédiable :

- Une crise **informatique** pouvant remettre en question la continuité et/ou la **pérennité** même de l'activité de l'entreprise
- Une crise de **communication** pouvant porter gravement atteinte à la **réputation** des dirigeants et/ou à l'image de l'entreprise
- Une crise **financière** pouvant grever durablement la compétitivité et/ou la **rentabilité** de l'entreprise

Chapitre 2 : La conception et la commercialisation du produit assurance des risques cybernétiques

Introduction

La cyber-assurance est un produit d'assurance visant à permettre à une entreprise d'être indemnisée des dommages immatériels qu'elle subit ou fait subir à un tiers du fait d'une introduction, suppression, altération ou vol de données sur son système d'information. Les polices d'assurance cyber offrent des prestations aussi variées que la prise en charge des indemnités financières après une attaque cyber jusqu'aux pertes d'exploitation.

Section 1 : Etude de marché

6. 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 est suivie d'un exercice de compilation permettant de présenter les données recueillies sous une forme récapitulative utile. Une enquête commence habituellement s'il y a un besoin d'information et s'il n'y a pas de données ou si elles sont insuffisantes. C'est parfois l'organisme statistique lui-même qui en a besoin ou un client à l'externe, peut être un ministère, un organisme gouvernemental ou un organisme privé. L'organisme statistique ou le client veut habituellement étudier les caractéristiques d'une population, assembler une base de données à des fins analytiques ou vérifier une hypothèse.

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 quinze questions réparties sur trois sections, chaque section se focalise sur un axe particulier de l'étude comme suit :

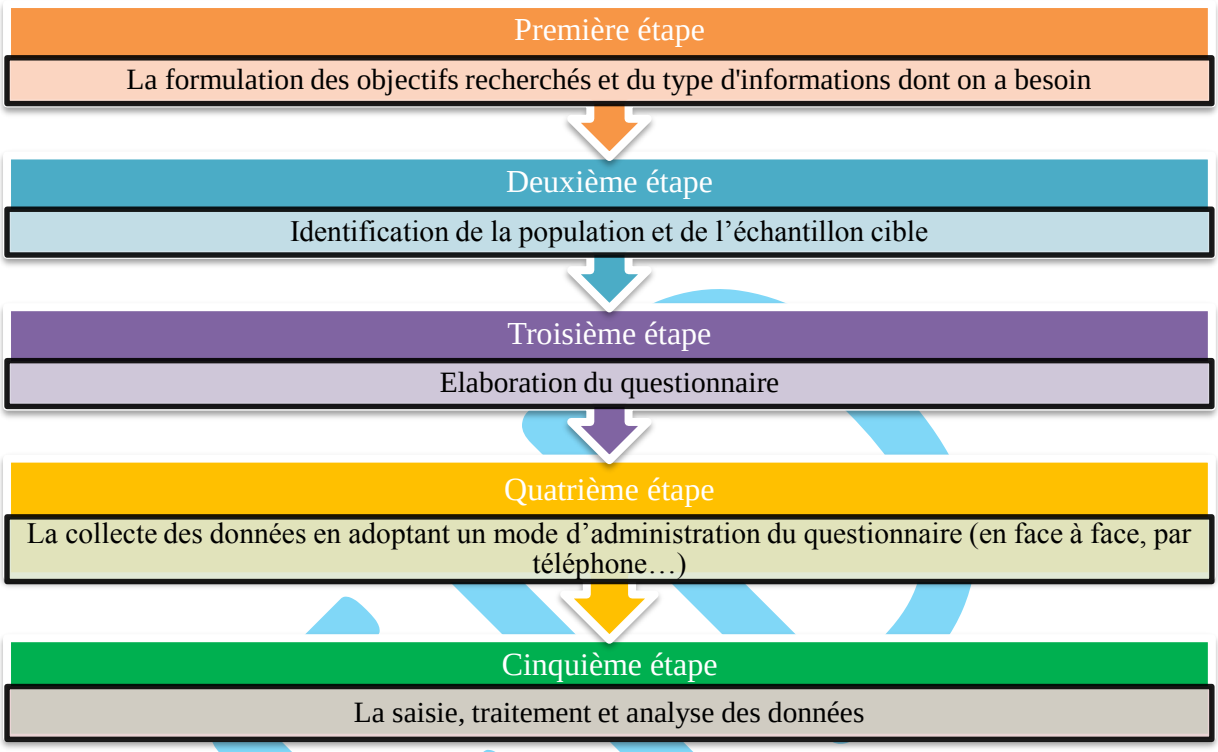
- La section A comporte quatre questions simples qui ont pour objectif de collecter quelques des informations générales :

- La deuxième section du questionnaire est destinée à évaluer qualitativement, et quantitativement si possible, le poids des incidents cybernétiques dans les banques à travers huit questions :
- Finalement, la troisième section, comportant trois questions, est dédiée à exposer l'offre du produit « Assurance des risques cybernétiques » pour dégager l'intérêt des parties concernées pour ce produit.

Le questionnaire serait alors diffusé aux 22 banques tunisiennes, 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 :

Banque
Union Internationale des Banques
Banque de Tunisie
Banque de l'Habitat
Union Bancaire pour le Commerce et l'Industrie
Amen Bank
Arab Tunisian Bank
Banque Tunisienne de Solidarité
Banque Nationale Agricole
Société Tunisienne de Banque
Attijari Bank
Banque Internationale Arabe de Tunisie (BIAT)
Banque de Tunisie et des Emirats (BTE)
Banque Tuniso Koweitienne
Tunisian Qatari Bank
Stusid Banque
Arab Banking Corporation
Banque Tuniso-Libyenne
Banque de Financement des Petites et Moyennes Entreprises
Banque Zitouna
Banque Franco-Tunisienne
Banque ALBARAKA
Wifack international bank
Bnaque centrale

Le questionnaire est envoyé sous forme d'un document Word contenant des cases cliquables pour les réponses à chaque question. La démarche de l'enquête est résumée dans ce diagramme :



7. L'analyse du questionnaire

L'échantillon prévu était de 22 banques mais vu la difficulté de joindre les responsables ciblés (Par email, sur place, par téléphone, à travers des anciens IFIDards, les enseignants de l'IFID et des contacts fournis par mon encadrant…) j'ai pu obtenir en totalité un nombre de 15 questionnaires remplis en bonne et due forme, sur lesquels je me suis basée pour faire les analyses nécessaires et dégager des résultats.

On va analyser les questions une par une selon leur ordre d'apparition dans le questionnaire après avoir créé une base de données sur **SPSS** (Statistical Package for the Social Sciences) et générer les statistiques et les graphes nécessaires à l'interprétation des résultats.

1.1.Informations générales :

1.1.1. <u>Veuillez évaluer les facteurs qui entraînent un changement important du niveau de risque cybernétique au cours des dix dernières années:</u>

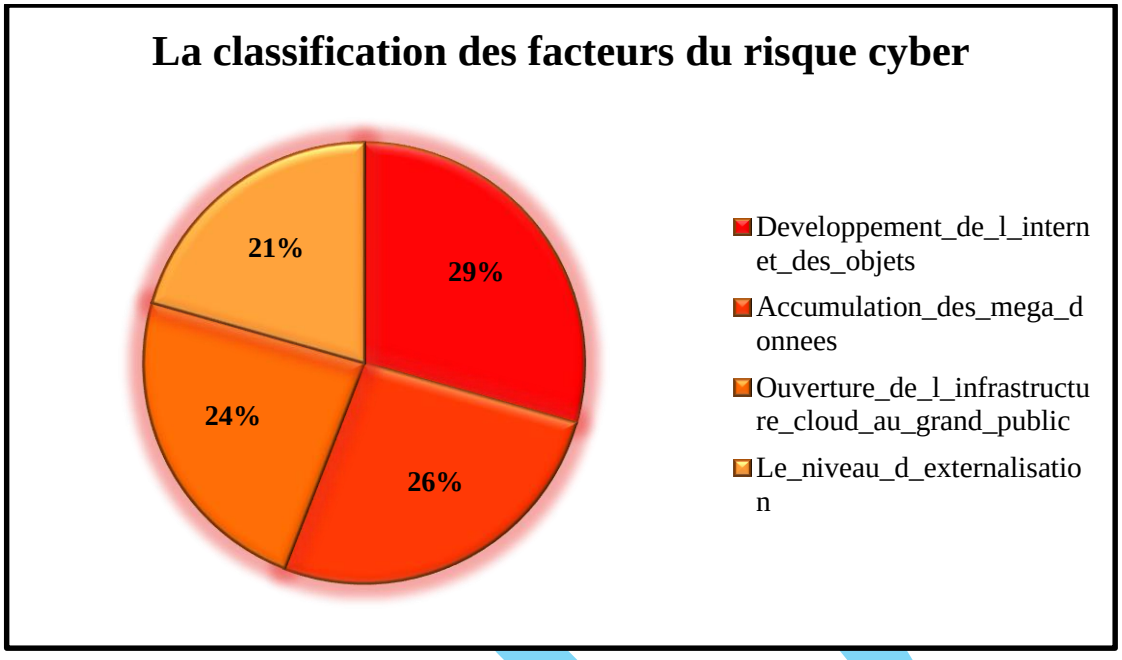


Figure 15: La classification des facteurs du risque cyber selon les banques

La réponse à la question posée consiste à évaluer quatre facteurs de risque que leur impact dans l'évolution des risques cyber est importante, modéré ou faible. Selon le camembert ci-dessus, on constate que **29%** des réponses favorisent l'importance du développement de l'internet des objets (Internet of things) ainsi que l'accumulation des méga données (big data), avec un pourcentage de **26%**, dans le développement des risques cybernétiques. L'ouverture de l'infrastructure cloud au grand public et le niveau d'externalisation viennent en dernier avec des pourcentages respectifs de **24** et **21%**.

Le développement de l'internet des objet a, évidemment, un impact énorme dans la prolifération 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 (les sites de location de voiture, les applications d'achat et de vente…) et la question qui se pose c'est : est-ce qu'on est vraiment prêt à ce développement exponentiel sur le plan sécurité informatique pour réduire au minimum la probabilité de l'occurrence des incidents cyber .

1.1.2. Considérez-vous que les entreprises tunisiennes sont menacées par des cyber-attaques /incidents? Si oui, veuillez évaluer le niveau de risque perçu

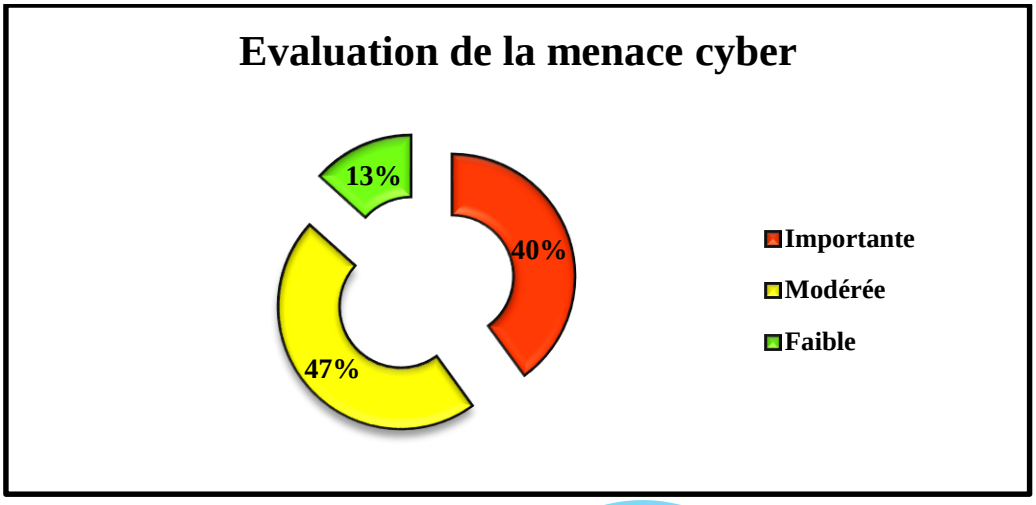


Figure 16: L'évaluation de la menace cybernétique

Le graphe dévoile que **40%** des interviewés considèrent la menace cyber comme importante, **47%** la considère comme modérée alors que **13%** 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.

1.1.3. Pensez-vous que les risques cyber ont évolué, plutôt, en termes de fréquence ou de sévérité ?

Dans la question précédente on a testé la conscience des interviewés, maintenant dans cette question on commence à décortiquer les dimensions de risque qui consistent en la sévérité et la fréquence.

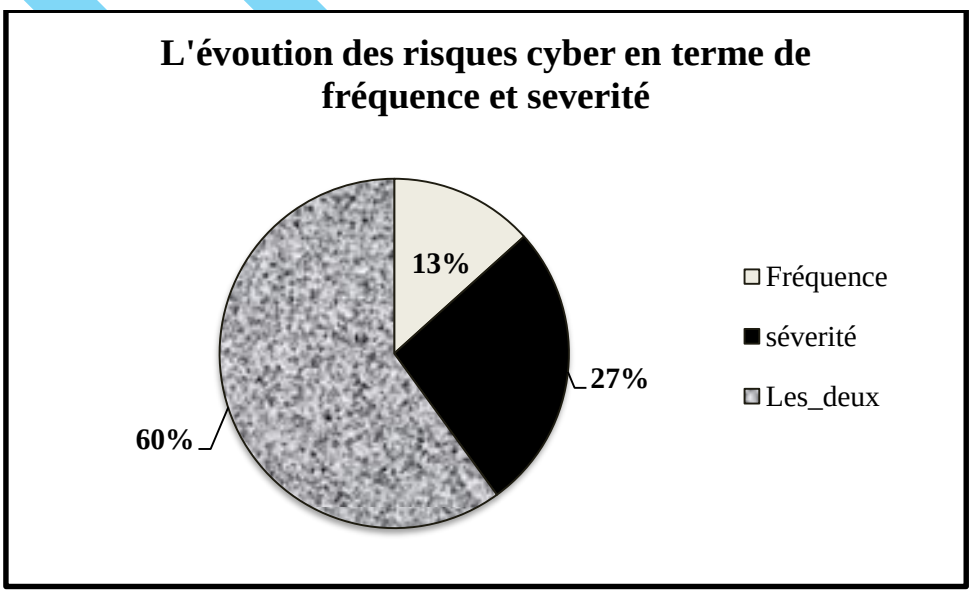


Figure 17: L'évolution des risques cyber en termes de fréquence et de sévérité

60% de l'échantillon confirment que les risques cyber évoluent non seulement en termes de sévérité mais aussi en termes de fréquence. Une bonne partie de 27% insistent aussi sur le fait que les risques cyber sont plutôt sévères que fréquents.

1.1.4. Quels sont les secteurs que vous jugez les plus exposés aux risques cyber ?

Cette question consiste à demander l'avis des banques concernant les secteurs les plus exposés au risque, les secteurs proposés sont :

-Le secteur financier

-Le secteur énergétique

-Le secteur militaire

-Le secteur technologique

Les résultats viennent alors comme suit :

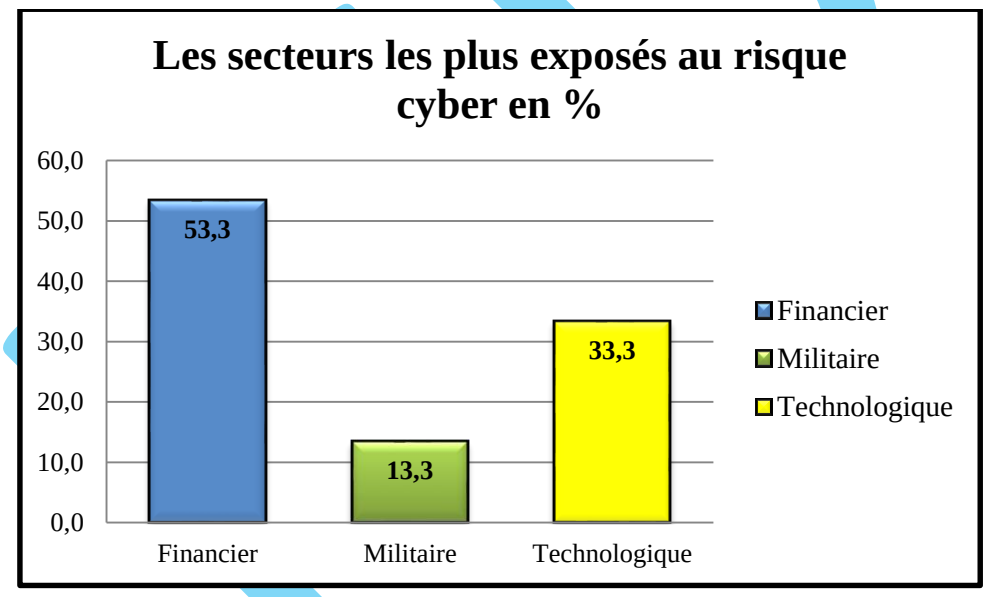


Figure 18: Les secteurs les plus exposés au risque cyber

53,3% des interviewés pensent que le secteur le plus exposé au risque est le secteur financier suivi du secteur technologique avec **33,3%**. Le secteur militaire avait été mentionné par **13,3%** des responsables contrairement au secteur énergétique que personne ne l'a mentionné.

On en déduit que les banques aperçoivent clairement le fait que le secteur financier est la cible numéro un des risques cybernétiques qu'ils soient intentionnels ou non vu la criticité de l'activité de ce secteur.

1.2.Le poids des risques cybernétiques :

1.2.1. Avez-vous été victime d'une attaque cyber ou d'une erreur informatique ?

C’est la question la plus critique de point de vue confidentialité, et pour favoriser les chances d’obtenir des réponses proches de la réalité **on** a ajouté une troisième option « Je ne peux pas répondre » qui crée une certaine nuance, **c’est un Oui déguisé**. D’ailleurs, comme le montre le graphe ci-dessous, **20%** des interviewés ont opté pour cette option, tandis que **33%** ont confirmé avoir été victime d’un incident cyber. En contrepartie, **47%** ont déclaré qu’ils n’avaient jamais été affectés par ce risque. On peut conclure, en quelque sorte, que 50% de l’échantillon étudié ont subi les dommages d’un incident cyber qu’il soit intentionnel ou non.

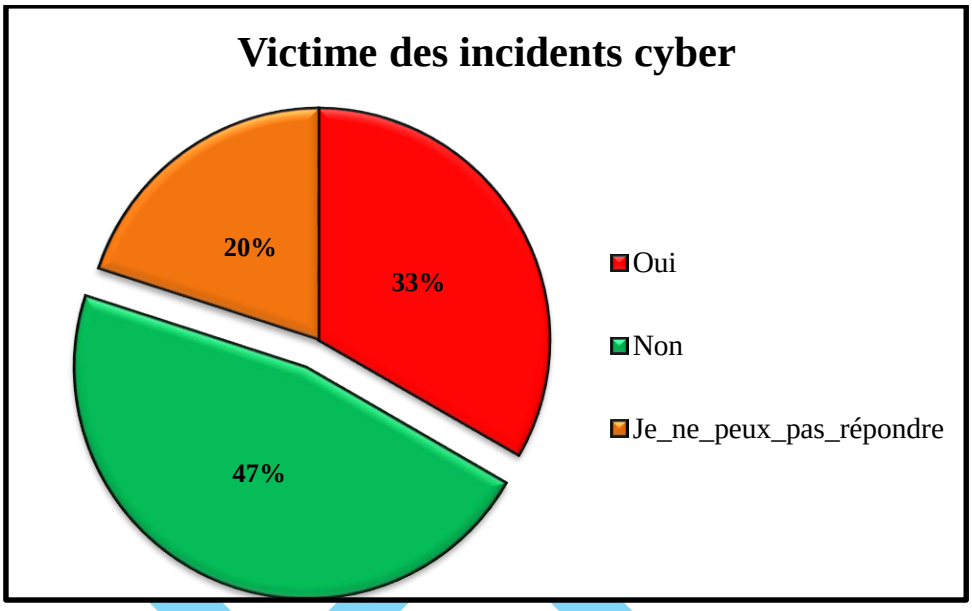


Figure 19: Avoir été victime ou non d'un incident cybernétique

1.2.2. Si oui pour la question B.1, quelles ont été les conséquences de cette attaque/erreur ?

Cette question est destinée à ceux qui ont confirmé avoir été victime d’un incident cybernétique. On a présenté ici, quatre types de pertes comme suit :

- Perte ou usurpation de données confidentielles (Relatives aux clients ou au personnel)
- Pertes d’exploitation
- Vol de propriété intellectuelle
- Atteinte à la réputation

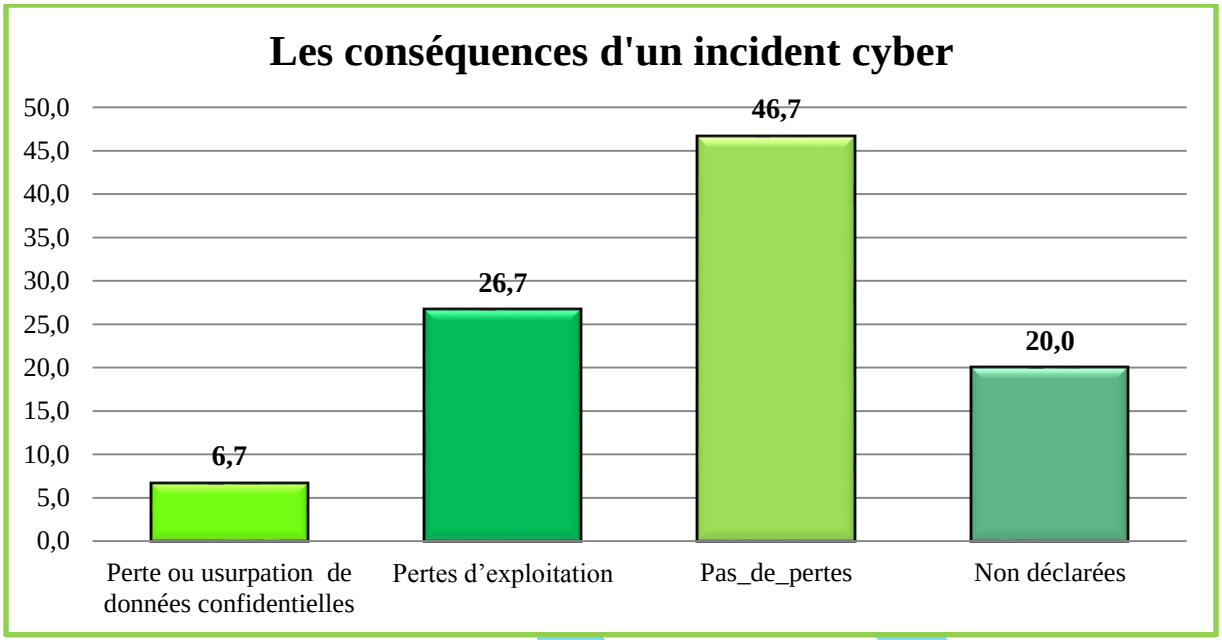


Figure 20: Les conséquences d'un incident cyber

Il y'a donc **6,7%** des interviewés victimes d'un incident cyber qui ont subi une perte ou usurpation de données confidentielles, **26,7%**, eux, ont subi des pertes d'exploitation, le reste, donc, est **46,7%** qui n'ont pas été touché par ce risque et **20%** qui n'ont pas exposé un avis clair concernant leur situation face au risque en question.

1.2.3. Si oui pour la question B.1, comment /combien quantifiez-vous la perte ?

Cette question vise à qualifier la perte (La quantifier si possible) par les interviewés qui avaient été atteints par un incident cyber.

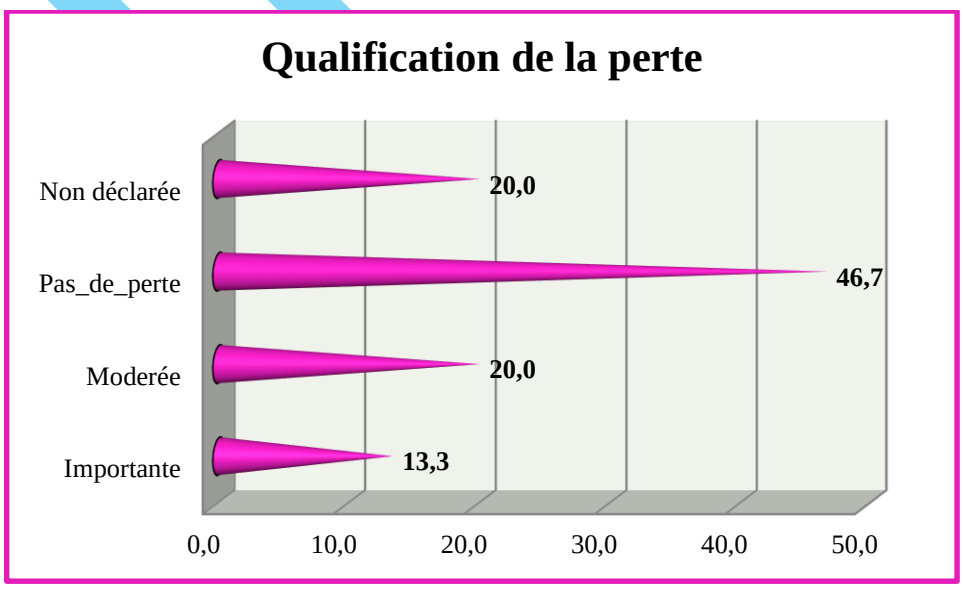


Figure 21: La qualification de la perte suite à une attaque cyber

On constate que **20%** des victimes ont qualifié la perte de « Modérée », tandis que **13,3%** l'ont considérée comme « Importante ». Les pertes subies par les **20%** sus mentionnés varient

entre 50000 dinars et 1 Million de dinars. (Seulement quatre interviewés ont donné un chiffre exact).

1.2.4. La performance du système de sécurité informatique de votre entreprise est jugée plutôt (Elevée/Moyenne/faible)

Par le biais de cette question on passe au volet sécurité informatique au sein des banques, on a commencé par juger sa performance :

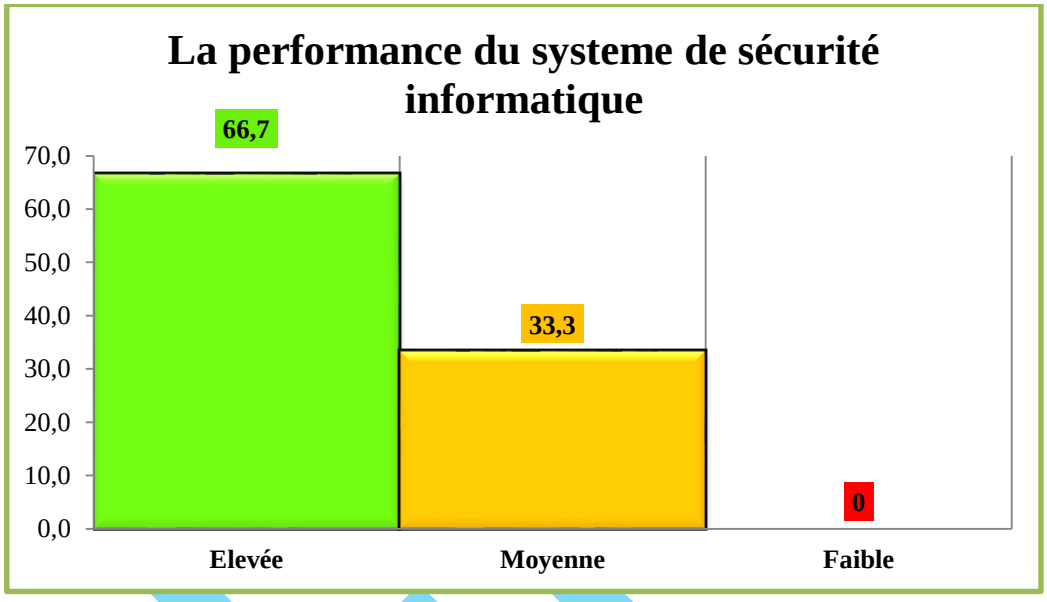


Figure 22: La performance du système de sécurité informatique de la banque

Le graphique ci-dessus montre que **66,7%** des banques interviewés affirment que le système de sécurité informatique au sein de leur société est bien performant, **33,3%** considère qu'il est moyennement performant tandis que personne n'a qualifié le système de sécurité de faible ou non performant. Ce jugement est plus ou moins relatif aux références de l'interviewé**, l'avis fourni ne peut pas être objectif.**

1.2.5. Quel est, à peu près, le montant investi annuellement dans la sécurité informatique (veuillez remplir le rectangle ci-dessous avec un montant approximatif)

Cette question confirme le fait que juger la performance du système de sécurité informatique est subjectif, en effet il y'a des interviewés qui ont affirmé l'allocation de montants énormes a la sécurité informatique et qui, en même temps, ont jugé la performance comme moyenne et vice versa.

D'abord on va exposer dans le graphique ci-dessous les chiffres fournis par les interviewés concernant les budgets investis en matière de sécurité informatique.

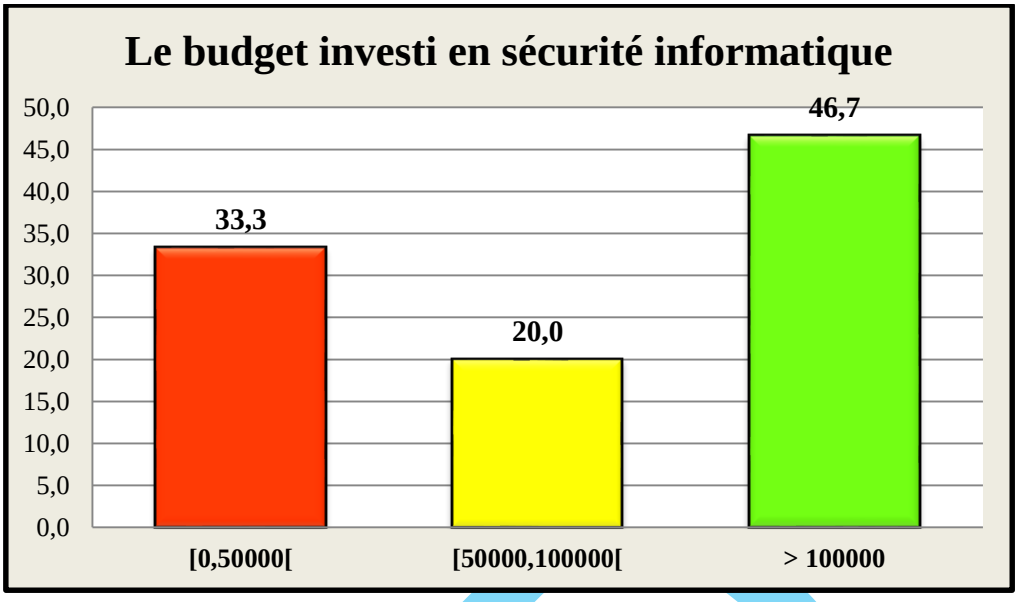


Figure 23: Le budget investi en matière de sécurité informatique

On constate que **46,7%** de l'échantillon en question ont fourni un chiffre qui est supérieur à 100K TND et **55,3%** ont délivré des chiffres inférieurs à 100K TND.

Ensuite, on veut tester la relation entre la performance du système de sécurité informatique et le budget investi en se basant sur un test qui tient compte des différentes natures des variables testées (Ordinale et métrique), c'est le test ANOVA choisi à l'aide de l'arbre de choix ci-dessous :

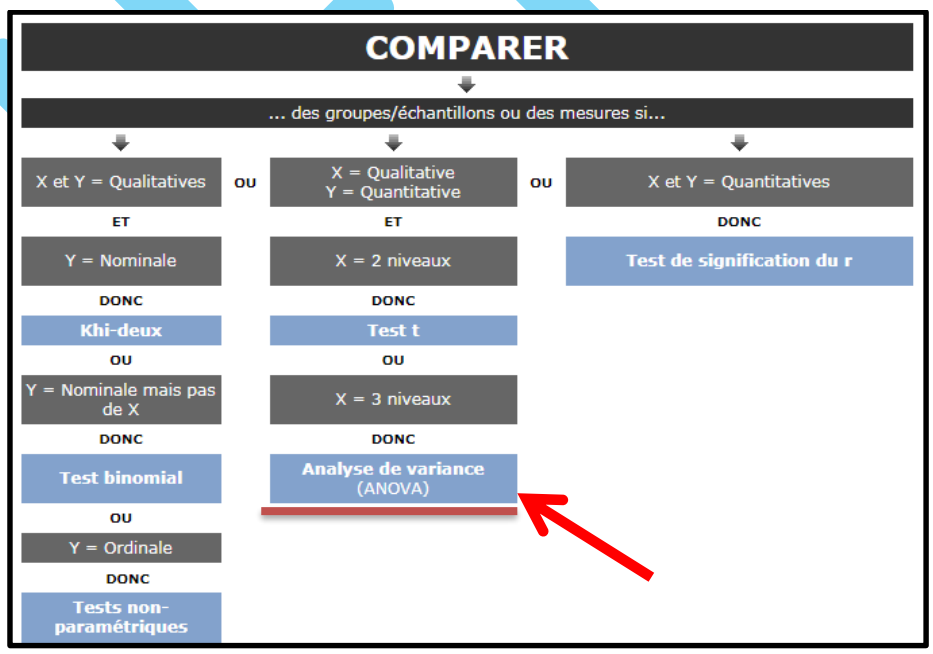


Figure 24: Arbre de choix des tests de comparaison sur SPSS

Tableau 3:Test de Khi-deux de la relation "performance du système de sécurité informatique et budget investi"

ANOVA

La_performance_du_systeme_de_sécurité_informatique

	Somme des carrés	ddl	Carré moyen	F	Sig.
Inter-groupes	2,833	10	,283	2,267	,224
Intragroupes	,500	4	,125		
Total	3,333	14			

Source : SPSS

Avec une simple analyse faite sur cet échantillon, à l'aide d'un test ANOVA sur SPSS, on peut déduire clairement que la relation entre la performance du système de sécurité informatique et le budget investi en la matière n'est pas significative (niveau de signification de 0,224> 0,05), ceci prouve ce qu'on a dit précédemment concernant les avis subjectifs qualifiant la performance du système de sécurité informatique dans la question (2.2.4.) (Ou bien ça prouve l'indépendance entre les deux facteurs : A vérifier)

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

C'est la seule question à laquelle tous les interviewés ont répondu par « Oui », ils confirment que la banque au sein de laquelle ils travaillent dispose d'au moins un expert en sécurité informatique. SPSS a considéré cette variable comme constante puisqu'on a la même réponse pour tout l'échantillon.

Tableau 4:L'existence d'un expert en sécurité informatique

Existence_d_au_moins_un_expert_en_sécurité_informatique

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	oui	15	100,0	100,0	100,0

Source : SPSS

1.2.7. 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 ?

60% des interviewés affirment que le personnel reçoit une formation continue et régulière en matière de sécurité informatique alors que **40%** (Un pourcentage que je vois énorme) ne sont

pas sensibilisés à la gravité de la menace cyber et ils **sont à côté** de la maitrise des moyens de sécurité afin de préserver les données confidentielles.

L'absence ou le manque de formation de personnel en ce sujet peut engendrer un risque opérationnel voir un risque frontière énorme.

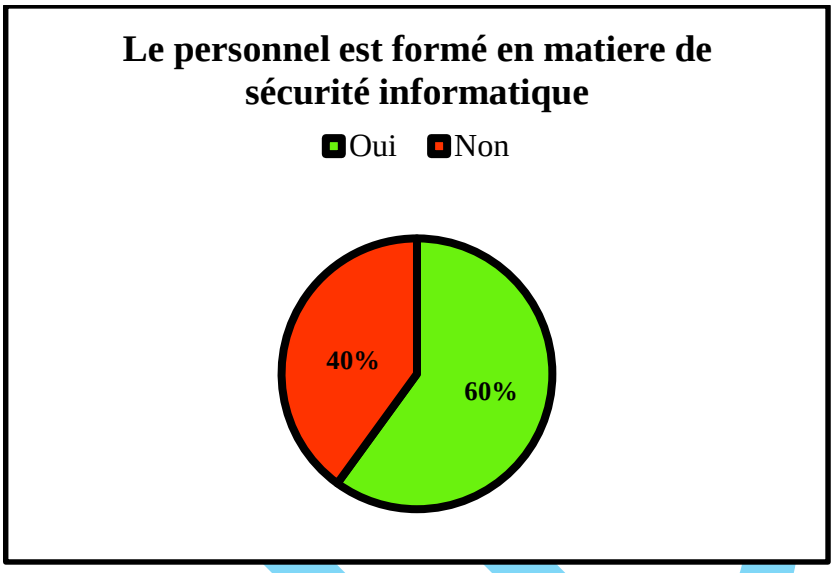


Figure 25: Le pourcentage du personnel informé au sein des banques

La relation entre la performance du système de sécurité informatique et la formation de personnel en la matière est forte et prouvée significative à l'aide d'un test Khi-deux effectué sur SPSS (Niveau de signification de **0,025< 0,05**). On a choisi le test Khi-deux car on veut tester l'influence d'une variable qualitative sur une autre variable qualitative. On a pu obtenir les résultats suivants :

Tableau 5: Test de dépendance entre la performance du système de sécurité informatique et la formation du personnel

Tests du khi-deux

	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	15				

Source : SPSS

1.2.8. Les ports USB des ordinateurs pouvant accéder aux données sensibles sont restreints ou désactivés :

Les espaces de stockage contenant des données sensibles et critiques peuvent faire face à des risques de l'installation des logiciels malveillants ou bien de vol de données. La majorité des attaques récentes ont été effectuées via les liens USB (Universal Serial Bus). Pour cette raison, on a posé cette question pour s'assurer que l'une des pratiques de sécurité les plus essentielles est appliquée au sein des banques. Dans ce contexte, **66,7%** des interviewés confirment avoir respecté cette mesure alors que **33,3%** confirment le contraire. Le fait que le **(1/3)** des banques ne procèdent pas à la désactivation des ports USB constitue une menace pour la sécurité de leurs système informatiques et favorise, autant, la présence des vulnérabilités.

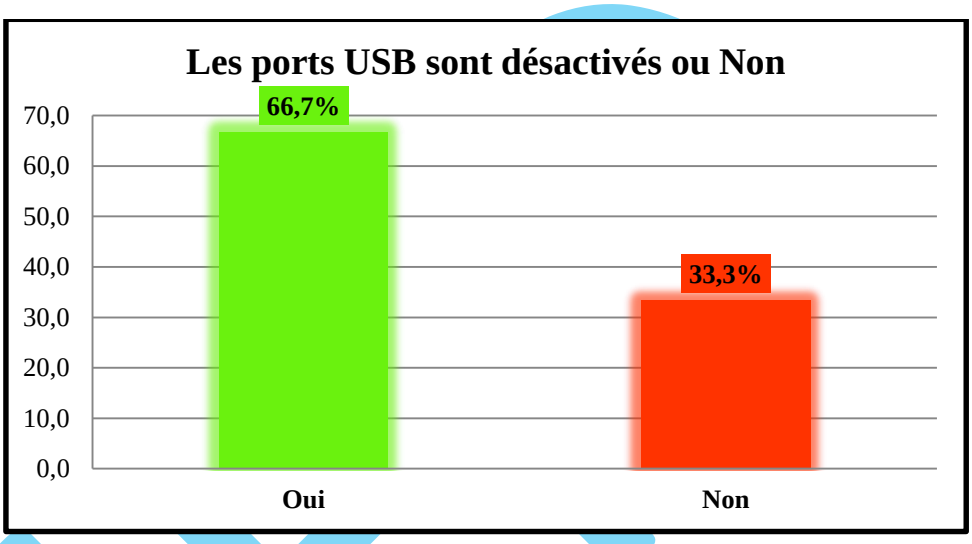


Figure 26: L'état des ports USB

C'était la dernière question de la deuxième section, passons maintenant à la troisième section du questionnaire.

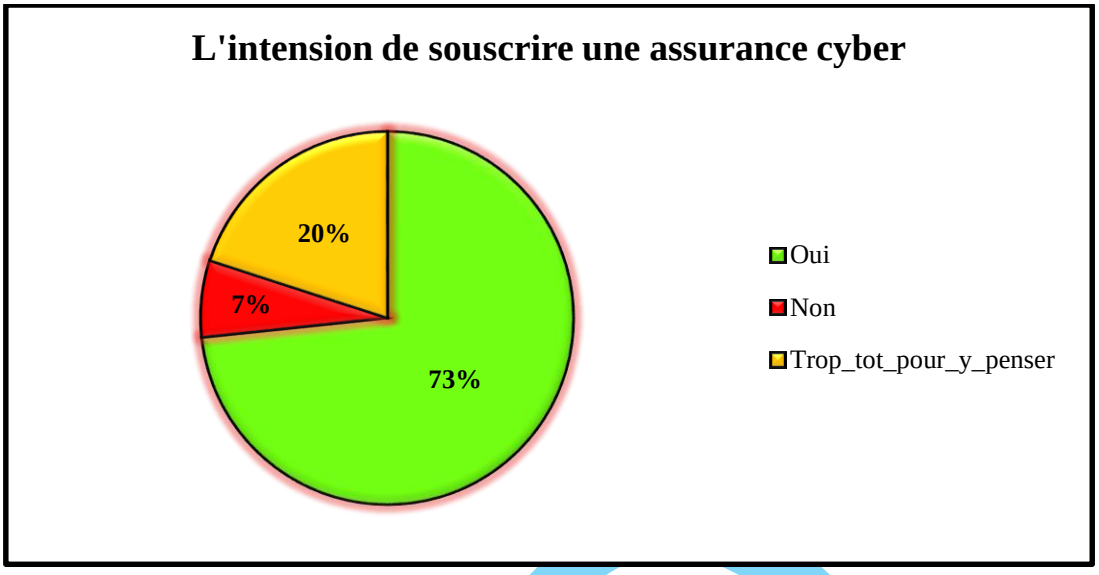
1.3.L'assurance des risques cybernétiques :

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

C'est la question clé du questionnaire à laquelle on peut répondre à travers trois options :

- Oui
- Non
- C'est trop tôt pour y penser

On a obtenu les résultats suivants :



Seulement **7%** des interviewés affirment qu'ils n'ont pas l'intention de souscrire une assurance cybernétique dans le futur. La majorité, **73%** ont montré un intérêt énorme à ce nouveau produit assurantiel, tandis que **20%** de l'échantillon croient que c'est une assurance futuriste et qu'on est encore loin de ce nouveau besoin mais ils sont convaincu, en même temps de l'importance de ce produit avec la révolution numérique et technologique.

Selon l'étude effectuée, il n'existe pas de lien direct entre le fait d'avoir été victime d'un incident cyber et l'intention ou la décision de souscrire une assurance cyber, ça peut refléter clairement un niveau de conscience élevé en ce qui concerne la nécessité de se prémunir de toute éventuelle perte même si on a pas vécu, avant, une perte pareille dans le cadre du principe « Mieux vaut prévenir que guérir ».

En effet, le test de dépendance Khi-deux a prouvé l'indépendance entre ces deux variables qualitatives comme le montre ce tableau :

Tableau 6: **Test de dépendance entre 'intention de souscrire une assurance cyber et le fait d'avoir eté victime d'un incident 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	15		

Source : SPSS

L'analyse d'indépendance à l'aide du test Khi deux indique que la prise de décision de souscrire une assurance cybernétique n'est pas influencée par le fait d'être une victime ou non

d'un incident cyber ce qui prouve la conscience « élevée » 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**.

On peut expliquer mieux cette indépendance à travers le graphique ci-dessous :

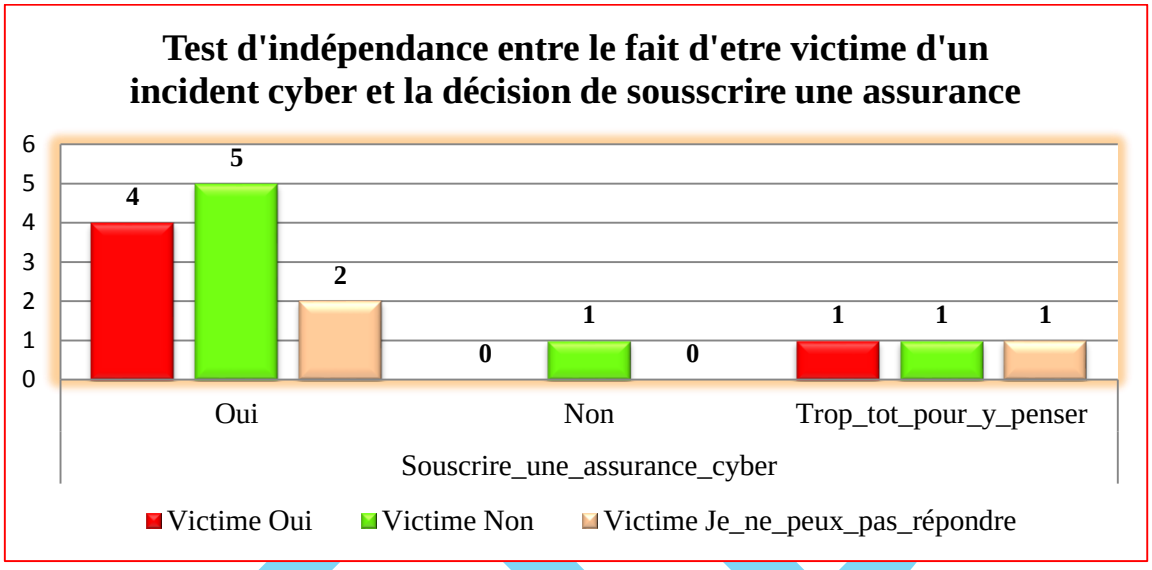


Figure 27:Test d'indépendance entre le fait d'être victime d'un incident cyber et la décision de souscrire une assurance

On remarque que le premier groupe contenant les interviewés qui ont l'intention de souscrire une assurance cybernétique est constitué de **4** personnes qui étaient victimes d'un incident cyber, **5** qui ne l'étaient jamais et **2** personnes qui pensent que c'est trop tôt pour penser à une assurance cyber. D'où l'indépendance entre la réalisation de l'incident et la décision de **souscription…**…

1.3.2. <u>Si oui pour la question C.1, quelles sont les couvertures que vous jugez utiles ?</u>

Dans cette question on demande aux interviewés de choisir une panoplie de couvertures directes et indirectes.

1.3.2.1.Couvertures directes :

On a proposé huit types de couvertures directes qui peuvent intéresser les interviewés :

- ✓ La 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 banque ainsi que les coûts de transmission de l'information aux actionnaires et aux clients. Elle couvre aussi les couts de restauration du Software (Tout ce qui est logiciel et systèmes d'exploitation).

- ✓ Les pertes d'exploitation :

C'est une couverture qui 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.

- ✓ La 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.

- ✓ La fraude :

C'est couverture qui 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…)

- ✓ Erreurs technologiques et omissions

Elle couvre toute suspension ou bien interruption du service fourni par le système informatique de la banque en cas d'erreur, négligence, omission ou tout acte non intentionnel exécuté par l'un des employés ou bien un prestataire de service lors de l'exploitation du système informatique au sein de la société.

- ✓ Détournements de fonds (Cyber-braquage)

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.

Pour le choix des couvertures directes on a obtenu les pourcentages suivants :

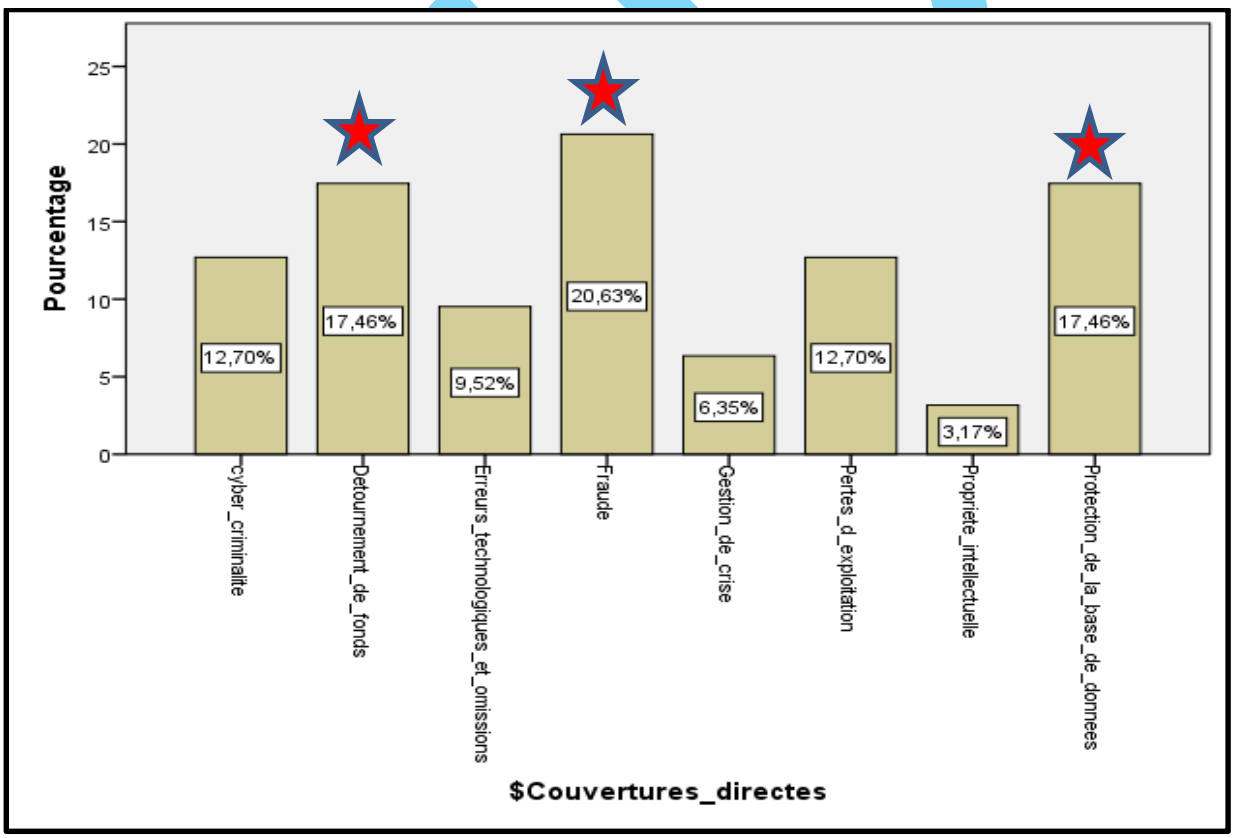


Figure 28: La sélection des couvertures directes par les interviewés

On constate que la couverture la plus demandée est celle qui couvre la fraude avec un pourcentage de **20,63%**, suivie, des couvertures contre la détérioration de la base de données et le détournement de fonds à pourcentages égaux de **17,46%**. La couverture la moins demandée par les interviewés est la protection de la propriété intellectuelle avec un

pourcentage de **3,17%**. On peut conclure donc que la fraude constitue le premier souci des banques en matière de cyber risques tandis que la propriété intellectuelle réside en dernier.

1.3.2.2.Couvertures indirectes :

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

- ✓ La responsabilité civile pour l'atteinte à la vie privée

Elle couvre principalement :

-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 (surveillance de la fraude ou autres services connexes aux clients et employés touchés par un cyber-événement)

-La protection contre le vol d'identité pour les clients

Elle couvre ces évènements suite à une divulgation d'informations confidentielles (informations nominatives, informations médicales confidentielles) collectées ou traitées par l'entreprise ou confiées à sa garde ou à son contrôle en raison de négligence, d'actes intentionnels, de perte, de vol par des employés, via un réseau informatique ou accès hors connexion.

- ✓ Responsabilité civile visant la sécurité de réseau

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 avoir de la sorte :

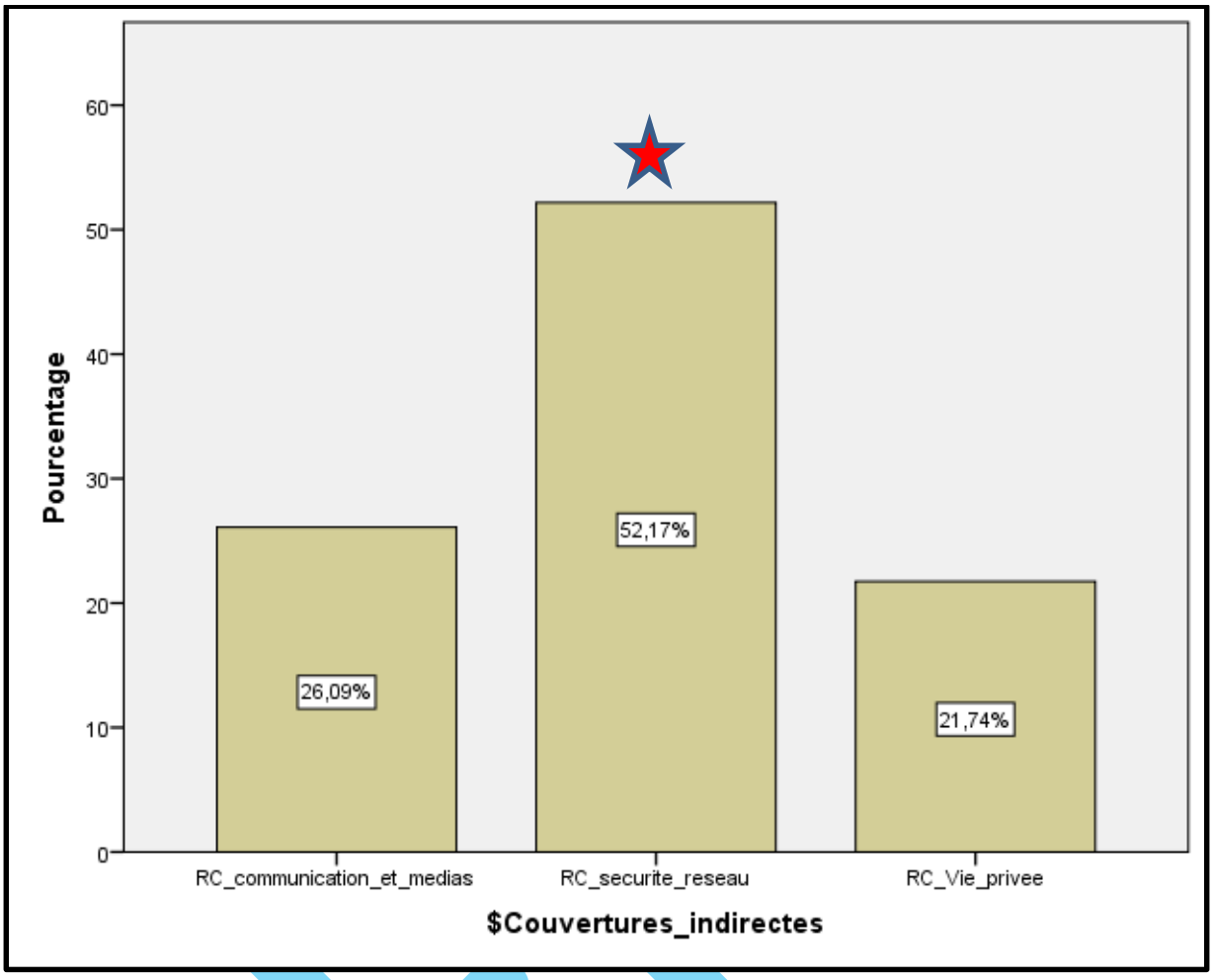


Figure 29: Le choix des couvertures indirectes

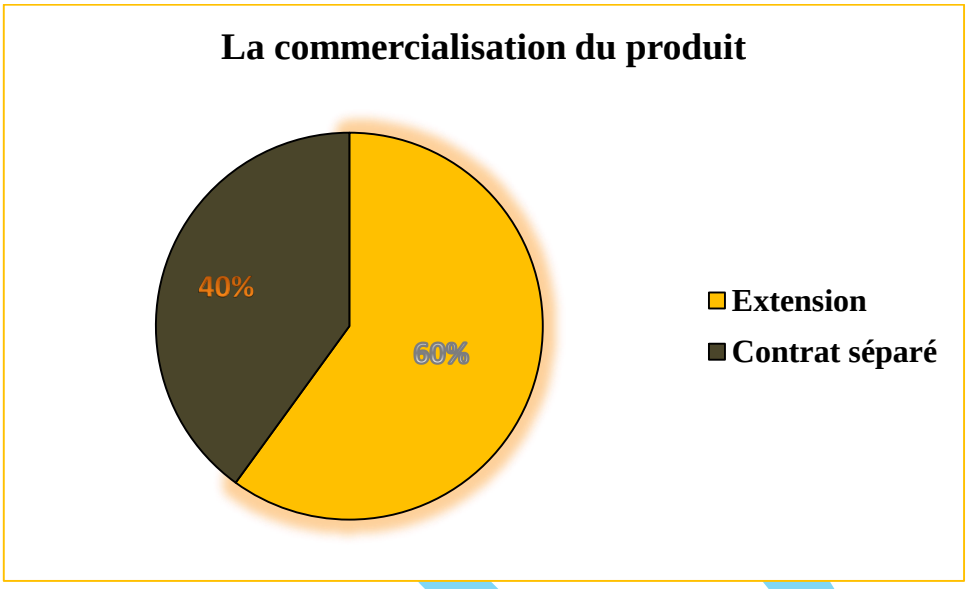
Leur premier choix était la responsabilité civile sécurité du réseau avec **52,17%** des avis. En effet, chaque entreprise est tenue de se prémunir à l'aide d'une protection des informations privées vu que plusieurs informations à caractère confidentiel existent dans leurs serveurs tels que les coordonnées, 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.

1.3.3. Préférez-vous, en tant que banquier, que l'assurance cyber, si elle existait, soit commercialisée :

Extension/ Contrat

C'est la dernière question de l'enquête, elle a pour objectif de déterminer le moyen de commercialisation le mieux adapté aux besoins des banques, c'est le fait de préciser la forme du packaging la plus acceptable par les consommateurs.

Les réponses à cette question viennent comme suit :



On a donc **60%** des interviewés qui préfèrent voir l'assurance des risques cybernétiques en tant qu'extension dans un contrat Globale des banques, alors que les **40%** restants optent pour un contrat séparé dédié à ce nouveau type d'assurance. Chacun des deux groupes a ses propres arguments, car, la distribution en tant qu'extension va certainement coûter moins cher alors que celle via un contrat bien structuré va être plus étendue avec une panoplie de choix plus vaste.

Pour résumer, les quinze questions analysées précédemment donnent un aperçu général sur l'état des banques en matière de cybersécurité et surtout sur leur acceptabilité vis-à-vis du produit « Assurance des risques cybernétiques ».

Section 2 : La conception du produit

1. Un contrat d'assurance des risques cybernétiques : Généralités

Le cybercrime génère un grand nombre de coûts. Les coûts directs comprennent les coûts relatifs aux rançongiciels, (des logiciels malveillants qui prennent en otage des données personnelles), à la perte de données et aux poursuites. Ce risque, s'il n'est pas assuré, peut faire perdre à des personnes leur emploi, argent et même réputation.

Les solutions technologiques veillant à contrer les cyberrisques ne sont pas multiples. La plupart des options que proposent les fournisseurs de sécurité informatique n'offrent pas la protection voulue et elles ne semblent pas s'améliorer assez rapidement et efficacement que les cyberrisques qui évoluent exponentiellement. En outre, ces contrôles techniques sont

généralement trop compliqués et très coûteux à mettre en place. Le manque de conscience et de la compréhension de la gravité des cyberrisques accentue le problème. Aussi, par manque de renseignements de sécurité, la majorité des entreprises semblent incapables de prendre des décisions sages liées à la façon de répartir leur budget, d'une façon optimale, en matière de cybersécurité.

Par conséquent, certaines entreprises se dirigent vers la solution la plus sure et la moins couteuse qui est la souscription d'une assurance cybersécurité. C'est en fait la décision de transférer le risque mieux que d'investir dans les solutions couteuses et qui ne garantissent jamais le risque zéro. En contrepartie, les assureurs sont tenus d'imposer des critères minimums de sélection des risques pour éviter le plus possible le fait que les entreprises soient imprudents à l'égard de ces risques qui sont très sensibles aux failles et aux erreurs humaines ce qui ramène les assureurs à améliorer , d'une part la culture du risque cyber chez les entreprises et d'autre part de sensibiliser et moraliser le risque chez eux pour éviter que ce risque soit subjectif . Deux raisons expliquent pourquoi les assureurs offrent une protection contre le cyberrisque :

- Premièrement : l'assurance responsabilité civile représente, pour de nombreux assureurs, une branche très importante et rentable.
- Deuxièmement : le cyberrisque est une branche d'assurance qui gagne en importance et qui ouvre de nouvelles possibilités de revenus. Un grand nombre des cyberrisques ne sont pas nouveaux tels que le vol de propriété intellectuelle, la perte de profits, le bris de confidentialité et l'atteinte à la réputation. Mais ça n'empêche les assureurs de créer de nouveaux produits et besoins en cyber sécurité.

2. Types de couvertures et étendues

   a. Couverture de base des risques cybernétiques :

****Couverture des risques propres**

Les polices d'assurance des risques cybernétiques couvrent généralement les sinistres subis par l'assuré, notamment la perte, le vol ou la divulgation non autorisée de renseignements confidentiels. Cette couverture inclut les frais engagés pour la notification de l'atteinte, les relations publiques, la surveillance du crédit, le centre d'appels et l'enquête judiciaire.

****Couverture des risques tiers**

Les polices d'assurance des risques cybernétiques couvrent aussi, généralement, les pertes de tiers provoquées par l'assuré, notamment les frais de défense, les dépens (les sommes qui sont dues finalement par la partie contre laquelle un jugement civil est intervenu) et les règlements.

b. Couvertures supplémentaires de la police d'assurance des risques cybernétiques :

****Protection contre les pertes d'exploitation**

Certaines polices d'assurance des risques cybernétiques peuvent fournir une protection contre les pertes d'exploitation découlant de l'interruption ou de l'arrêt du système informatique de l'assuré à la suite d'une atteinte à la sécurité du réseau.

****Cyberterrorisme**

Aujourd'hui, les cyberattaques parrainés par un État sont l'une des sources extérieures d'atteinte à la vie privée qui connaissent la plus forte croissance au sein des entreprises.

Malheureusement, les polices d'assurance des risques cybernétiques n'ont pas toutes évolué de manière à reconnaître cette source grandissante de risques; en fait, de nombreuses polices contiennent toujours les exclusions de « guerre » et de « terrorisme », ce qui pourrait influer sur la couverture des pertes découlant de ces attaques.

Certains assureurs sont disposés à accorder des exceptions à ces exclusions, afin de préciser qu'ils n'excluent pas la couverture des actes de Cyberterrorisme. Ce type d'exception devrait être incorporé à chaque police d'assurance des risques cybernétiques contenant des exclusions de « guerre », de « terrorisme » ou d'autres exclusions similaires.

****Dommages corporels et matériels**

Quasiment toutes les polices d'assurance des risques cybernétiques excluront les dommages corporels et matériels imputables aux cyberattaques et aux atteintes à la vie privée. Dans certains cas, l'exclusion s'étend aux sinistres en souffrance morale et en trouble émotif, ou en découlant.

Cette large exclusion des dommages corporels et matériels pourrait être problématique, étant donné qu'un demandeur pourrait exiger des dommages-intérêts à plusieurs niveaux, notamment des dommages-intérêts pour souffrance morale et trouble émotif.

**** couverture des procédures réglementaires**

Certaines polices d'assurance des risques cybernétiques prévoient une couverture des enquêtes et procédures réglementaires. Toutefois, comme le libellé n'est pas uniforme, la couverture de certaines polices est plus robuste que d'autres.

La majorité des polices incluent la couverture des frais de défense engagés dans le cadre des procédures réglementaires, d'autres polices plus exhaustives couvriront également les amendes et les sanctions, sous réserve de leur assurabilité en vertu de la loi.

3. Les exclusions

1. **Les sinistres rendus possibles par l'absence de système de protection antivirus et firewall mis à jour régulièrement et activé en permanence, ou par une défaillance dans la protection de système informatique non remédiée dès la prise de connaissance.**

2. **Les sinistres successifs dus à une même cause, pour autant que des recommandations en matière de prévention pour éviter la reproduction du sinistre vous aient déjà été notifiées, mais n'aient pas été mises en œuvre dans un délai maximum de 6 mois suivant la date de formulation de ces recommandations.**

3. Les sinistres résultant de l'utilisation de logiciel acquis illégalement, sauf si son utilisation l'est à votre insu.

4. Les sinistres résultant de la collecte illicite de votre part, de données tiers, ou de données personnelles ou confidentielles.

5. Les frais d'amélioration de votre système informatique, des programmes et données, ou de votre système de protection contre les intrusions malveillantes.

6

Les sinistres résultant de tout fait dommageable ou évènement : – dont vous aviez connaissance à la date d'effet des garanties du présent contrat, – visé dans toute enquête ou procédure amiable, administrative, judiciaire, pénale ou arbitrale antérieur, à la date d'effet des garanties du présent contrat.

Section3 : L'enjeu de la tarification

1. La difficulté de tarification pour les risques cyber

La cyber-assurance est potentiellement une énorme opportunité de croissance, mais pour l'exploiter de manière rentable, les entreprises doivent identifier et quantifier les cyberrisques.

L'attitude à l'égard de l'assurance cyber change. Ceci est partiellement dû à la prise de conscience croissante des violations de sécurité majeures. L'assurance cyber est désormais considérée comme un élément fondamental dans la gestion des risques cybernétiques.

Bien que les risques cyber présentent pour les assureurs des opportunités considérables, ces derniers sont confrontés à une réalité dure : La quantification précise du cyberrisque 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.

✓ **Défis de prix**[9]

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

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

- 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:

- Un environnement des affaires en pleine évolution
- Evolution 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. Mais se tromper peut avoir de sérieuses implications, à la fois pour l'activité de l'assureur et pour le marché dans son ensemble.

- ✓ **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.

- ✓ **Quantification des inconnues avec une approche holistique**

La combinaison des obstacles discutés jusqu'ici a bloqué le développement de méthodes vraiment complètes pour la modélisation des cyberrisques. En conséquence, le prix des primes reste inexact. Cela a empêché une plus grande adoption de l'assurance cybernétique en tant qu'élément efficace de la gestion des risques. Cette situation incite les assureurs à retenir des positions conservatrices lors de la tarification des contrats et à appliquer des limites de garanties.

Un paysage dynamique, tel est le danger cyber, nécessite une réponse dynamique. Cela doit inclure la surveillance de la qualité et la performance du système de sécurité en temps réel et la quantification dynamique des risques. Pour adopter des changements positifs, les actuaires et les souscripteurs doivent se focaliser sur des points importants, tels que:

- La compensation du non disponibilité des statistiques à travers les tests de résistance (Stress tests/ scénarios)
- L'incorporation de la sécurité dérivée d'experts et de renseignements propres à l'industrie
- La mise en œuvre de technologies de pointe, y compris l'apprentissage automatique.

Les menaces cybernétiques continuent à se développer dans l'avenir, les opportunités commerciales dans le domaine de la cybersécurité continuent de croître. L'offre de produits et de primes de cybersécurité appropriés, accessibles et abordables est essentielle à ce marché en croissance. Mais cela n'arrivera que lorsque l'innovation et la recherche seront mises en œuvre. La législation a, aussi, un rôle clé à jouer, en promouvant la normalisation des politiques et en aidant à préparer le passage d'un marché limité en matière de cybersécurité à un marché structuré, bien réglementé et offrant des offres de masse.

La complexité de la procédure de tarification peut être diminuée dans l'avenir si on applique toutes les directives liées à la cybersécurité. Toutes les institutions doivent déclarer, en détail, les circonstances des incidents auxquels elles étaient victimes afin de bien valoriser et quantifier le risque cyber. Le manque de transparence ne peut qu'impacter négativement les assurés et les assureurs.

Actuariellement, le risque cyber se trouve à la limite du champ de l'assurable et il peut fuir les modèles de tarification les plus sophistiqués. En effet, d'une part, ce type de risque est caractérisé par un niveau de perte catastrophique pareil à celui des catastrophes naturelles qui semblent plus maitrisées grâce aux statistiques, à l'expérience et aux données géographiques et météorologiques. D'autre part, il y'a un autre facteur qui vient s'ajouter à la liste des contraintes de tarification et qui est un peu spécifique aux risques cybernétiques celui de l'interdépendance ou de la corrélation des risques.

A l'intensité spectaculaire des risques cyber et leurs interdépendance s'ajoute aussi l'insuffisance d'historique sur les sinistres survenus et leurs impacts financiers du fait de la discrétion des entreprises sur les circonstances et l'impact des incidents subis ainsi que l'évolution exponentielles du e-business donc des transactions en ligne. Plusieurs contraintes se réunissent pour inhiber le déroulement de la procédure de tarification en bonne et due forme.

Jusque-là, les estimations du coût du cyber assurance pour les différents types d'entreprise sont plus ou moins « spéculatives »10.

Afin de modifier la perception des entreprises concernant les cyberrisques encourus, il faut passer, impérativement, par éveiller leur conscience des conséquences économiques qui peuvent affecter la sérénité de l'entreprise en l'absence d'une couverture assurantielle adaptée en matière du risque cyber. Il est primordial, donc, de sensibiliser les différents acteurs économiques et surtout de médiatiser les sinistres.

Le partage et la divulgation de l'information sur l'état de sécurité, les incidents subis, les montants des pertes… augmentent remarquablement le degré d'aversion au risque. Les entreprises peuvent bénéficier d'un « effet direct » de la divulgation d''information sur leur demande d'assurance cyber et d'un « effet stratégique » sur les prix.

De ce fait, il faut penser à la mise en place des centres de collecte d'informations afin de réduire les incertitudes et faire connaitre mieux les cyberrisques par toutes les parties concernées et plus particulièrement les banques, qui constituent une cible séduisante pour ce type de risque. Le pouvoir public doit obliger les entreprises à partager leurs expériences dans ce domaine.

[10]Charles d'AUMALE, François GRATIOLET, Stéphane SOLLAT& François-Xavier VINCENT.2017. *Comment « débloquer » le marché de l'assurance cyber en France.* Telecom Paris Tech

2. La chaine cybercriminelle : CYBER KILL CHAIN (CKC)

Malgré la difficulté et la complexité de la tarification des cyberrisques, les incidents de cybersécurité peuvent être modélisés de façon stochastique par **l'Analyse de Markov** qu'on détaillera par la suite**.**

En effet, les facteurs qui sont à l'origine des incidents de cybersécurité sont appelés la : **Cyber Kill Chain (CKC)**. Cette dernière expose les sept stades d'une attaque cybernétique, chaque stade exige la réussite de la précédente :

Tableau 7 : Les sept stades du cyber kill chain

Reconnaissance	Armement	Livraison	Exploitation	Installation	Commandement et contrôle	Attaques ciblées
						

Chaque stade du processus consolide le stade précédent ou en tire avantage. Toute rupture de la chaîne bloque l'attaquant. La CKC s'inspire de la méthode créée par le ministère américain de la Défense pour décrire la structure d'une attaque[11].

Vu que chaque étape de la Cyber Kill Chain dépend de l'échec de celle qui la précède, on peut modéliser les incidents cyber de façon stochastique à l'aide de l'analyse de Markov comme moyen de quantification de la probabilité de défaillance d'un système de sécurité sur une période donnée ou un nombre d'attaques. On définit ci-dessous les sept stades de la CKC :

- ✓ La reconnaissance :

C'est le premier stade, là où les attaquants effectuent une recherche minutieuse afin d'identifier et choisir les cibles. Ils essayent de collecter les adresses mail, les comptes rendus diffusés (des conférences, séminaires, formations…) , les relations via les réseaux sociaux et toutes les informations précieuses et nécessaires sur la victime pour pouvoir passer à l'étape suivante.

- ✓ L'armement :

[11] Eric M. Hutchins, Michael J. Cloppert et Rohan M. Amin, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, livre blanc, Lockheed Martin Corporation.

C’est la création de l’arme, l’attaquant attache un logiciel malveillant à une charge livrable, tel qu’un document PDF ou WORD généralement à l’aide d’un outil automatique appelé « **Weaponizer »**.

- ✓ La livraison :

La transmission de l'arme à l'environnement ciblé. Les trois vecteurs de livraison les plus répandus sont les pièces jointes, les sites Web et les supports amovibles USB.

- ✓ L’exploitation

Une fois le logiciel malveillant est installé dans le réseau informatique de la victime, le code des intrus est déclenché et activé et commence à chercher une vulnérabilité (faille) dans un logiciel, une application ou bien un système d’exploitation.

- ✓ L’installation

Les intrus tentent d’avoir accès en installant dans le système un cheval de Troie ou une porte dérobée. Dans un logiciel, une porte dérobée (backdoor), c’est une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel. L'introduction d'une porte dérobée dans un logiciel à l'insu de son utilisateur transforme le logiciel en cheval de Troie.

- ✓ Le commandement et le contrôle :

Le système infecté rappelle l’ordinateur des attaquants en établissant le commandement et le contrôle.

- ✓ Les attaques ciblées :

Seulement maintenant, après avoir progressé au cours des six premières phases, les intrus peuvent prendre des mesures pour atteindre leurs objectifs. Généralement, cet objectif est l'extraction de données ce qui implique la collecte, le cryptage (Le chiffrement ou cryptage est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de chiffrement.) et l'extraction d'informations de l'environnement de la victime. Alternativement, les intrus peuvent utiliser la victime initiale pour passer à d’autres victimes potentielles à l'intérieur du réseau.

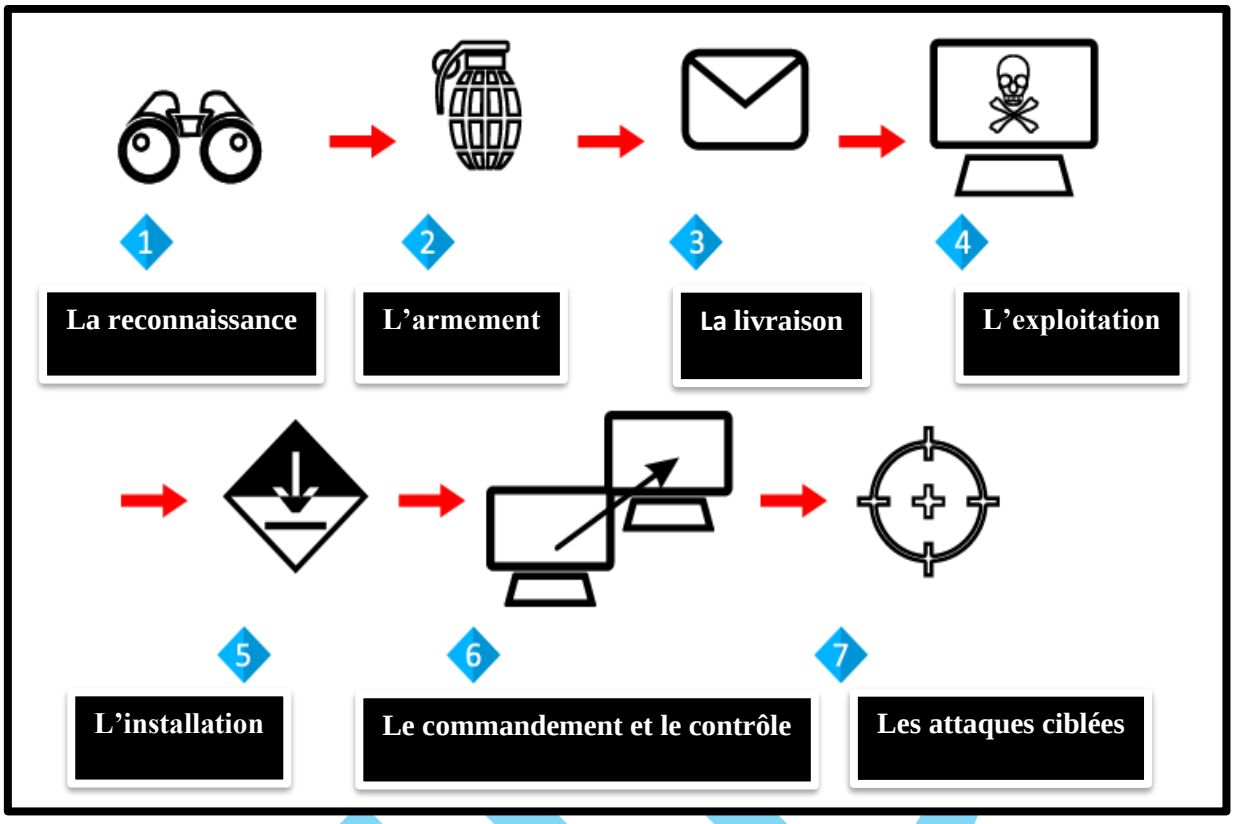


Figure 30: Schéma explicatif de la chaine cybercriminelle

Pour chaque stade, il y'a des processus et des outils spécifiques à la sécurité de l'information qui permettent de repérer les intrusions douteuses. On est donc capable de déterminer la probabilité qu'un attaquant puisse réussir à échapper aux moyens de sécurité mis en jeu.

Même pour les deux premiers stades qui se déroulent et se préparent hors du réseau informatique de la victime, on est toujours capable d'estimer la probabilité de défaillance ou de réussite de l'attaque. En effet, les systèmes responsables à la détection des intrusions sont capables de contrôler et vérifier le balayage de ports au cours des deux premiers stades. En outre, l'utilisation de l'analytique web serait efficace dans la détermination si un attaquant est en train de collecter des informations clés.

3. L'analyse de Markov : Le principe simple

L'analyse de Markov est utilisée pour de nombreux types de calculs de la fiabilité, pour lesquels une suite d'événements dépendants peut entraîner des défaillances du système

Un type d'analyse de Markov est appelé chaîne de Markov. 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 (voir figure 2). 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.

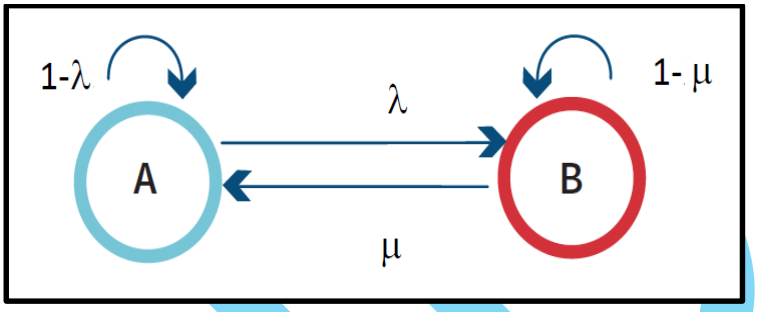


Figure 31: Simple diagramme de transition d'états de la chaine de Markov

Nous pouvons construire une matrice de transition à partir de ce diagramme (figure 17). 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 :

$$\begin{bmatrix} \mathbf{1-\lambda} & \boldsymbol{\lambda} \\ \mu & \mathbf{1-\mu} \end{bmatrix}$$

1-λ : La probabilité de rester dans l'état A

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

μ : La probabilité de rester dans l'état B

1-μ : La probabilité de passer de l'état B à l'état A

Suite à une succession de passage par plusieurs états, la probabilité de se présenter dans certain état est indiquée par cette équation :

$$x_t = x_0 \times P^t$$

Avec :

x : est le vecteur d'état du système

x_0 : est le vecteur d'état initial du système

P : La matrice de transition

4. Calcul de la probabilité d'une faille de cybersécurité : Application de la chaine de Markov au cyber Kill Chain :

L'analyse de Markov peut être appliquée au cyber Kill Chain afin de calculer la probabilité de défaillance d'un système de sécurité. Dans ce qui suit on va utiliser un exemple de calcul simple pour illustrer cette analyse à l'aide 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.

Par exemple, un mécanisme correctif consiste à corriger une vulnérabilité dans un système d'exploitation. Pour mieux comprendre le principe, nous allons examiner seulement deux stades. Dans l'exemple qui suit, la chaîne de Markov de la Cyber Kill Chain est définie pour le passage de l'état (1) à l'état (3) en recourant aux deux stades suivants : La **livraison** et l'**exploitation**.

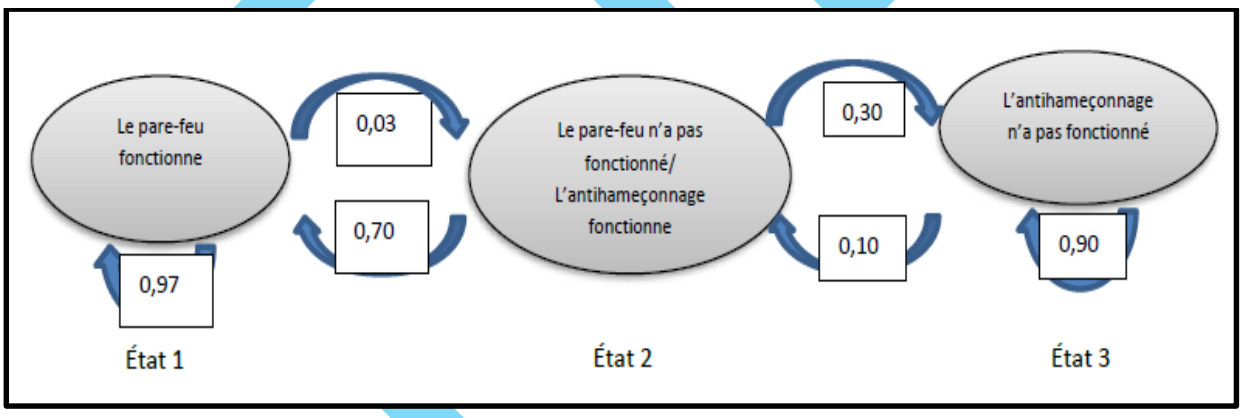


Figure 32: Diagramme de transition du cyber kill chain

*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 (.exe) 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 18 illustre la probabilité de ces états à l'aide d'un diagramme de transition La chaîne de Markov peut être appliquée à la CKC pour calculer la probabilité de défaillance d'un système de cybersécurité. Nous utiliserons ici un simple exemple et des probabilités statiques relatives aux composants individuels.

La sécurité de l'information est contrôlée par des mécanismes de prévention, de détection et de correction.

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.

Par exemple, un mécanisme de correction consisterait à apporter un correctif à un système d'exploitation vulnérable. Pour simplifier l'exemple, nous examinerons seulement deux stades.

La chaîne de Markov de la CKC est définie pour le passage de l'état 1 à l'état 3 en recourant aux deux stades suivants : livraison et exploitation.

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 .exe 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 4 illustre la probabilité de ces états à l'aide d'un diagramme de transition.

$$P = \begin{bmatrix} 0,97 & 0,03 & 0 \\ 0,7 & 0 & 0,3 \\ 0 & 0,1 & 0,9 \end{bmatrix}$$

Et le vecteur d'état initial est donné par $\mathbf{x_0}$**= [1 0 0]**. Après **100** cycles, le vecteur résultant est $\mathbf{x_{100}}$ **= [0,853 0,036 0,109]**. En d'autres termes, la probabilité que le logiciel malveillant soit exécuté est d'environ **11 %** (c'est-à-dire que la probabilité d'être dans l'état 3 est de 0,109).

Le modèle CKC nous permet de regrouper en une suite logique les divers outils et processus utilisés en cybersécurité. Une fois établie cette suite logique, l'analyse stochastique de la fiabilité peut être utilisée pour calculer la probabilité de défaillance.

Dans cet exemple, nous avons utilisé un modèle très simple avec des probabilités statiques. Nous utiliserons des probabilités plus complexes et plus rigoureuses lorsque nous aurons mieux compris les taux de fiabilité des divers outils de sécurité. En outre, les entreprises divulguent plus souvent qu'auparavant des données sur les menaces informatiques dont elles sont l'objet. Un meilleur échange de données entre les entreprises sera pour beaucoup dans la compréhension des taux de fiabilité des outils de protection cybernétique.

Comme nous l'avons vu, l'application d'une méthode de calcul de la fiabilité aux systèmes de cybersécurité peut faciliter la quantification de la probabilité d'une défaillance d'un système de protection cyber. Une fois estimée la probabilité de défaillance, l'analyse actuarielle utilisée à l'égard des produits d'assurance pourrait être appliquée aux systèmes informatiques.