**Information security breaches and financial market reaction: the French case**

 Pauline MENDIELA

 ESSCA

**Abstract**

This study examines the impact of information security breaches on the stock returns on French companies. Using the event study methodology, we provide insights on the effect of cyberattack announcements on the market value of French companies from 2009 to 2019. We show that following cyberattack announcements, stock returns significantly decrease. We find that financial companies are more negatively impacted than other industries. Our results lead conclude that cybersecurity is now fully integrated into risk management and the overall strategy of companies. Cyber resilience appears to be the essential element to face current threats and reassure investors.

**Keywords**

Cybersecurity; Market reaction; Stock returns; Event Study

**Résumé**

Cette étude examine l’impact des atteintes à la sécurité de l’information sur les rendements boursiers des entreprises du marché boursier français. À l’aide de la méthodologie de l’étude d’événements, nous fournissons des données sur l’effet des annonces de cyberattaques sur la valeur marchande des entreprises de 2009 à 2019. Nous montrons que des rendements négatifs se produisent à la suite d’annonces de cyberattaques. Nous constatons que certains secteurs d’activité subissent souvent des effets négatifs plus importants que les autres entreprises, c’est notamment le cas des entités financières. Nos résultats nous amènent à penser que la cybersécurité est aujourd’hui pleinement intégrée à la maîtrise des risques et stratégie globale des entreprises. La cyber résilience apparaît être l’élément essentiel pour face faire aux menaces actuelles et rassurer les investisseurs.

**Introduction**

Cybersécurité, système d’information, faille de sécurité, virus, cyberattaque, ransomware, hameçonnage et résilience sont autant de mots préoccupant les directions des risques des grandes entreprises françaises. Le développement des technologies de l'information affecte tous les secteurs économiques. Si Internet a souvent permis d’améliorer de bien des manières notre quotidien, il a également augmenté la vulnérabilité des infrastructures pour atteindre et compromettre la sécurité de l'information. La cybercriminalité coûte de plus en plus cher aux entreprises avec une augmentation de 72% du coût moyen des attaques sur l’année 2018 (Accenture, 2019). Le nombre de cyberattaques n’a cessé de croître ces dernières années. Si en 2017, plus de 19 millions de Français ont été concernés par des attaques informatiques (Norton 2017), les attaques en 2019 ont été tout aussi nombreuses et impactantes.

Alors que la plupart des attaques informatiques avaient un faible impact il y a quelques années, la sophistication de certaines d’entre elles ayant récemment touché de nombreuses entreprises a attiré l’attention tant des professionnels que des particuliers. L’augmentation des atteintes à la sécurité au cours des dernières années, l’inter connectivité des réseaux et la nécessité de collecter toujours plus de données ont suscité un intérêt grandissant pour la cybersécurité au sein des organisations. Ce nouvel enjeu de sécurité est défini par l’ANSSI comme « l’état recherché pour un système d’information lui permettant de résister à des évènements issus du cyberespace, susceptibles de compromettre la disponibilité, l’intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu’ils rendent accessibles ». Dans ce contexte, la cybersécurité cherche donc à défendre tous les systèmes numériques, qu’ils soient connectés entre eux ou non, tels que les systèmes liés à l’Internet des objets2.

Ainsi, le risque lié aux systèmes d’information et la protection de ces derniers sont devenus en peu de temps une préoccupation majeure poussant les entreprises à faire évoluer leurs stratégies en matière de gestion des risques. Ces risques sont à la mesure des enjeux puisqu’aujourd’hui, une cyberattaque ou une erreur non intentionnelle de manipulation de données peut compromettre la confidentialité, l’intégrité et l’accessibilité de données et de systèmes d’information. Elle peut également se solder par de lourdes pertes financières, et aller jusqu’à menacer la survie d’une entreprise ou le fonctionnement et la sécurité d’un État.

En 2017, les attaques WannaCry et NotPetya ont rappelé les menaces que le risque cyber fait peser sur l’économie et la société. Face à cette multiplication des incidents de grande ampleur, les petites et grandes entreprises tentent, à leur échelle, de développer des environnements cyber résilients. Ainsi en 2018, 76%5 (Ernst & Young, 2018) des entreprises mondiales déclarent avoir augmenté leur budget alloué à la cybersécurité, tentant ainsi de minimiser les risques liés aux attaques. Ces atteintes aux systèmes d’information représentent des coûts implicites et explicites non négligeables (Gordon et Loeb, 2011) dont d’importantes pertes financières. La cybercriminalité apparaît alors comme une préoccupation majeure des actionnaires, qui par manque de confiance, déplaceront leurs capitaux et par conséquent impacteront la valeur de marché de l’entreprise et sa capacité à financer son développement.

Depuis quinze ans, plusieurs études se sont intéressées à l'impact des annonces de faille de sécurité des systèmes d’information sur la valeur marchande des sociétés cotées en bourse aux Etats Unis et dans le monde. La valeur marchande représente la confiance que les investisseurs ont dans une entreprise, et la mesurer est un moyen de calculer l'impact d'une cyberattaque. En outre, Bener (Bener, 2000) affirme que le comportement des investisseurs dépend de ce qu'ils ont observé dans le passé, c'est-à-dire que les investisseurs prennent des décisions en fonction de l'impact des atteintes à la sécurité de l’information d'une entreprise dans le passé. Plusieurs études (Campbell, 2003; Cavusoglu, 2004; et Hovav et D'Arcy, 2004) utilisent la méthodologie de l'étude d'évènements pour estimer les conséquences des cyberattaques sur la valeur marchande des entreprises ayant été compromises.

Contrairement aux évènements ou annonces positives qui produisent souvent des rendements bénéfiques, les évènements découlant de failles de sécurité et/ou cyberattaques sont généralement considérés comme des indications d'une mauvaise gestion des processus technologiques, des infrastructures et plus généralement de la stratégie globale. Nous pouvons donc penser qu’ils ont un impact négatif sur la valeur marchande des entreprises. Cependant, après analyse des résultats de précédentes études sur ce sujet ce constat reste mitigé et peu concluant.

Ainsi Campbell et coll. (2003) sont parmi les premiers à utiliser la méthodologie d'analyse d'évènements pour analyser les réactions des marchés boursiers aux annonces de violations et failles de sécurité dans les systèmes d’information des entreprises. Après avoir examiné le cours des actions de 43 sociétés cotées en bourse, les auteurs ont constaté qu'il n'y avait aucune preuve statistique pouvant appuyer l'hypothèse de réaction négative globale du marché boursier. En revanche, l'étude a révélé un rendement négatif très important du marché lorsque l’atteinte portait sur la sécurité de données confidentielles de façon non autorisée. Toutefois, la petite taille de l'échantillon (seulement 11 incidents liés à des données confidentielles) ne permet pas de généraliser ce constat à toutes les entreprises notamment dans les entreprises du marché français. Dans une seconde étude, Garg et coll.. (2003) ont analysé vingt-deux atteintes à la sécurité informatique survenues entre 1996 et 2002. Leurs résultats publiés ont pu démontrer que les entreprises qui ont subi ces atteintes ont connu des rentabilités négatives anormales par rapport au marché. Une étude similaire, mais plus approfondie a été réalisée par Cavusoglu et coll. (2004). Bien que leur étude soit plus récente et ait une taille relativement plus grande que les études précédentes avec près de soixante-six évènements analysés, les incidents de l'échantillon sélectionné datent de la même période, soit entre 1996 et 2001. Les auteurs ont trouvé des rendements anormalement négatifs par rapport au marché pour l’ensemble de l’échantillon dans une fenêtre de deux jours. Ils ont également constaté des rendements négatifs plus importants pour les entreprises du e-commerce et les entreprises à faible capitalisation boursière. La fenêtre d’analyse de jours proches de l’évènement paraît être décisive et refléter les réactions des investisseurs à ces annonces. L’étude ne montre cependant pas de fenêtre d’analyse suffisamment grande pour pouvoir constater avec certitude si l’effet de l’annonce s’estompe ou non. De plus, il était intéressant de constater à cette période, symbole des prémices du e-commerce, que ces entreprises étaient plus vulnérables. Cependant, sur la période actuelle, presque toutes les entreprises proposent des biens ou services à la vente sur internet. Analyser uniquement l’échantillon sous cet angle semblerait moins pertinent.

De plus, Hovav et D'Arcy (2003) ont suivi une méthode similaire à la précédente étude, mais n'ont enquêté que sur les attaques DoS. Ils n'ont trouvé aucun résultat permettant d’appuyer l'hypothèse de réaction négative du marché boursier suite aux annonces. À cette occasion, ils s’étaient appuyés sur un échantillon réduit en analysant uniquement vingt incidents. Lors d’une étude ultérieure, impliquant un échantillon beaucoup plus vaste de 186 attaques de virus, Hovav et D'Arcy (2004) n’avaient de nouveau pas pu dégager une tendance claire. Cependant, les résultats de cette étude peuvent être faussés par la nature des attaques. En effet, les virus les plus virulents affectent souvent un grand nombre d'entreprises simultanément ce qui peut rendre l'analyse des évènements moins efficiente. Lors d’attaques de grande ampleur, comme ce fut le cas en 2017 par exemple, il est fort probable que les postes de travail et systèmes d’information touchés, appartenant à des sociétés cotées en bourse, ne soient pas individuellement impactés sur leur cours de bourse. L’effet de masse a pu réduire l’inquiétude et la perception négative des investisseurs.

Enfin en 2018, un groupe de chercheurs (Kamiya et coll. 2018) ont également analysé les réactions du marché à l'annonce de cyberattaques. Ils s’attendaient à ce qu'une cyberattaque soit coûteuse pour une entreprise, car susceptible de conduire à des dépenses sur les systèmes d’information, de faire face à des frais de litiges et amendes. Par conséquent, à ce que les entreprises subissent une rentabilité anormalement négative à la suite des différentes annonces. Conformément à cette attente, ils ont constaté un rendement anormal cumulatif moyen (RCA) significatif de 0,84 % au cours d’une période de trois jours entourant les annonces de cyberattaques. Avec une valeur marchande moyenne d'environ 58,93 milliards de dollars pour leur échantillon, cette baisse de rendement s’est traduite par une perte de valeur moyenne de 495 millions de dollars par attaque. Ils ont également constaté que les entreprises ayant fait face à des attaques entraînant une perte d'informations financières personnelles, leur RCA moyen est de 1,09%.

Après lecture et étude de différentes analyses, nous constatons alors que les résultats sont mitigés : les annonces ont souvent, mais pas nécessairement, eu un impact négatif significatif sur le rendement des actions. (Hovav et D’Arcy, 2003,2004 ; Kannan, 2007 ; Winn and Govern, 2009 ; Brockett, 2012 ; Shackelford, 2012). Cavusoglu (Carvusoglu, 2004) constate que les entreprises qui ont subi une attaque perdent en moyenne 2,1 % dans les deux jours suivant l'annonce. Acquisti, (Acquisti, 2006) montre que les atteintes à la protection des données ont un impact négatif et statistiquement significatif sur la valeur marchande d'une entreprise le jour de l'annonce. Enfin, d’autres études constatent de significatives réactions dans les dix jours suivant l’annonce de faille de sécurité.

Les résultats divergent notamment en fonction de la taille de l’échantillon et à la nature des évènements de sécurité impactant ainsi la cohérence globale de la méthodologie d'analyse des évènements. Les échantillons de trop petite taille peuvent se révéler non significatifs cependant, il n’est pas toujours évident de pouvoir détecter ce type d’incidents notamment avant les années 2000. Il s’avère que la littérature s’attardant uniquement sur la rentabilité des actions suite à une annonce de faille portant atteinte à la sécurité des systèmes d’information sur le marché des entreprises de la Bourse de Paris est très peu développée. De même, le marché boursier européen ne fait pas l’objet d’étude spécifique bien qu’il paraisse parfaitement adapté et intégré à la fois dans un processus de développement du numérique et du cyberespace. Il apparaît également intéressant de mener cette étude sur une période durant laquelle l’exposition aux cyber menaces n’a cessé de grandir et durant laquelle les entreprises ont consacré de plus en plus de budgets et de temps à la maîtrise de ce risque. C’est également depuis quelques années que les investisseurs et clients de ces entreprises se sont familiarisés avec le risque cyber, qu’ils y ont été sensibilisés et formés. Il se peut donc que cette recherche apporte des résultats plus forts quant aux rentabilités anormales des entreprises ayant subi ces préjudices. De plus, bien que tous les secteurs soient aujourd’hui la proie de ces menaces, certains sont plus attrayants que d’autres. Ils collectent plus de données à fort potentiel comme les données personnelles sensibles sur les clients dans le secteur de la santé et de la finance. Bien que ces secteurs soient de plus en plus réglementés en France et en Europe et que les entreprises déploient de plus en plus de moyens en matière de gestion de risque cyber, ce dernier n’est jamais écarté.

Enfin, notre étude s’attardera uniquement à l’analyse des cours boursiers suite aux évènements collectés contrairement aux précédentes études (Kamiya et coll., 2020 ; Amir, 2018) qui ont considéré les impacts également sur des éléments fiscaux. C’est dans ce contexte que nous chercherons à répondre à cette question : Quel est l’impact d’une annonce publique de faille de sécurité informatique sur la rentabilité d’une entreprise cotée sur le marché boursier français ?

## Hypothèses

Suite à l’analyse des précédentes littératures, il ressort que les résultats ne sont pas toujours cohérents bien qu’assez souvent un impact négatif sur la valeur marchande des entreprises soit observé sans être pour autant très significatif. Plusieurs facteurs ont pu influencer ces résultats notamment les facteurs méthodologiques sélectionnés dans les études antérieures. Globalement, les études sur les évènements de faille de sécurité informatique sont basées sur de petits échantillons. En effet, ce n’est que très récemment que les entreprises françaises et européennes ont des obligations légales de déclaration de ce genre d’incident. Auparavant, les entreprises évitaient au maximum de laisser s’ébruiter ce genre de nouvelle qui pouvait quoiqu’il arrive nuire à l’image de l’entreprise et avoir de nombreux impacts négatifs. De plus, certaines études se sont focalisées sur un type d’attaque en particulier comme les virus (Hovav et D’Arcy, 2004).

Aujourd’hui, réaliser une étude uniquement sur les attaques et infections de poste par virus ne pourrait plus se révéler efficace tant les attaques ont évolué, se sont complexifiées et sophistiquées. De nombreuses études analysant les rentabilités anormales de la valeur d’une action se sont basées sur l’hypothèse d’efficience des marchés avancée par Fama en 1970. Ainsi, selon ce modèle, il est admis que les investisseurs prennent en considération toute l’information disponible et évaluent la valeur de l’entreprise en tenant compte de ces facteurs. Lorsqu’une nouvelle information intervient, comme une annonce de faille de sécurité, ces derniers recalculent la valeur de l’entreprise. Ainsi, cette différence représente la variation de valeur de l’entreprise qu’a entraînée l’information rendue publique. Nous pouvons alors comprendre que la réaction des marchés boursiers aux annonces d’évènements est le reflet de la perception des investisseurs quant au potentiel futur de l’entreprise. Ce modèle appliqué aux failles de sécurité informatique permettrait d’avancer que suite à une annonce, les investisseurs considéreraient la faille comme une menace potentielle pour les performances futures. Ces annoncent pourraient également entraîner d’autres coûts divers pouvant impacter la capacité de l’entreprise à produire des bénéfices à court et moyen terme. Enfin, les failles de sécurités peuvent être directement perçues par les investisseurs comme une menace puisque l’entreprise apparaît alors incapable de protéger correctement ses systèmes d’information et toutes les données plus ou moins confidentielles qu’ils contiennent. Ces constats premiers nous permettent de poser la première hypothèse, à savoir :

**Hypothèse n°1 :** Une atteinte à la sécurité des systèmes d’information d’une entreprise entraîne une rentabilité anormalement négative de la valeur de ses actions lorsqu’elle est rendue publique.

Les failles de sécurité vont également impacter la perception des clients et utilisateurs des services relatifs proposés. Ces derniers peuvent alors remettre en question l’efficacité, la fiabilité et la capacité des systèmes d’information, des outils déployés tels que les pare-feu et systèmes anti- intrusion. Ces lacunes témoigneront d’une mauvaise gestion de la sécurité aux yeux des clients et d’une potentielle menace pour leurs données personnelles. Cette perte de confiance laisse entrevoir une mauvaise gestion stratégique et globale de l’entreprise en question pouvant entraîner une perte de confiance des parties prenantes. De plus, nombre d’entreprises collectent et détiennent des données très sensibles sur les collaborateurs, prospects, clients et processus internes ou nationaux. C’est le cas notamment des entreprises du secteur de l’armement, du médical, de la finance et des énergies. Cependant, il n’est pas rare que ces entreprises aient dû faire face à diverses attaques ces dix dernières années, parfois réussies et non sans conséquence. Ainsi, nous pouvons annoncer la seconde hypothèse, à savoir :

**Hypothèse 2 :** Une atteinte à la sécurité des systèmes d’information d’une entreprise entraîne une rentabilité anormalement négative sur la valeur de ses actions lorsqu’elle est rendue publique en fonction de son secteur d’activité.

De plus, ces dernières années les attaques se sont multipliées, complexifiées et ont eu des impacts de plus en plus importants. Face à ces enjeux, chaque acteur a dû se saisir de ces phénomènes et mettre en place des mesures parfois imposées et réglementaires ou non. En mai 2018 est entré en vigueur le Règlement Européen sur la Protection des Données (RGPD). Il harmonise les règles et les pratiques européennes, applicables en matière de protection des données à caractère personnel. Il concerne les entités publiques ou privées, établies dans l’UE ou touchant des personnes dans l’UE, les entreprises de toutes tailles, administrations et collectivités qui traitent des données à caractère personnel sont concernées. (ANSSI, 2018).

Aujourd’hui, les entreprises européennes ont donc en partie l’obligation de déclarer aux autorités compétentes lorsqu’elles ont fait l’objet d’une atteinte aux données personnelles qu’elles possédaient et peuvent être sanctionnées pour ces faits. Les clients et investisseurs devraient donc quelque part se sentir rassurés par ces mesures et les investissements réalisés par les entreprises. Ainsi, notamment pour mettre en conformité les systèmes et processus métiers, les dépenses en cybersécurité progressent trois fois plus vite que la dépense informatique totale avec une perspective de +8,6% en 2020. (IDC, 2019)

Cependant les entreprises peuvent subir différents types d’atteintes et failles de sécurité ne touchant pas systématiquement des données personnelles. Depuis dix ans, les types d’atteintes à la sécurité ont été très variés. Chaque atteinte peut avoir des conséquences différentes en fonction des entreprises et objectifs de l’attaque. Outre les atteintes aux données personnelles qui sont à présent sanctionnées, l’accès non autorisé aux informations confidentielles des entreprises devrait lui aussi entraîner des répercussions négatives, quel que soit le type. Cependant, les études précédentes n’ont pas toujours permis d’affirmer cette supposition malgré l’application de méthodologies différentes. Par exemple, Campbell et coll. (2003) ont regroupé les atteintes à la sécurité en données confidentielles et non confidentielles, et ont gardé les vols de données d'employés, de données d'entreprise et de clients dans un groupe comme confidentiel, tandis Cavusoglu et coll. (2004) ont utilisé un autre système en divisant les atteintes à la sécurité informatique en deux catégories : les attaques de déni de service et toutes les autres. Cette analyse nous amène à avancer une troisième et quatrième hypothèse, à savoir :

**Hypothèse 3 :** Une atteinte à la sécurité des systèmes d’information d’une entreprise entraîne une rentabilité anormalement négative de plus ou moins grande importance sur la valeur de ses actions lorsqu’elle est rendue publique en fonction du type d’atteinte aux systèmes d’information.

**Hypothèse 4 :** Une atteinte à la sécurité des systèmes d’information d’une entreprise entraîne une rentabilité anormalement négative de la valeur de ses actions lorsqu’elle est rendue publique en fonction du type de données touchées ou ciblées.

Enfin, malgré le peu de recul que nous avons sur les évènements, il est intéressant de comparer l’impact des cyberattaques au début de la période sélectionnée et à la fin de cette dernière. Ces dix dernières années, les usages liés à Internet, à l’Internet des objets, à l’intelligence artificielle a évolué de manière exponentielle. Toutes les infrastructures des réseaux informatiques se retrouvent en interconnexion et exposés. Tous les secteurs professionnels sont concernés par ces évolutions. Les autorités ont également saisi l’importance de ces changements et le cadre réglementaire ne cesse de se transformer pour maîtriser tout ce qu’engendre l’accroissement du cyber espace et de ses menaces. Il est alors intéressant de s’attarder, dans cette étude sur les rendements anormaux constatés au début de notre période d’analyse et ceux constatés en fin de période. En effet, cette fin de période est clairement caractérisée par la prise de conscience généralisée de ces menaces et la volonté de réglementer toutes ces pratiques. Peu d’acteurs peuvent aujourd’hui ignorer le risque cyber, considéré comme risque systémique et majeur aux yeux de toutes les directions d’entreprises.

**Hypothèse 5 :** Une atteinte à la sécurité des systèmes d’information d’une entreprise entraîne une rentabilité anormalement négative si elle a eu lieu ces deux dernières années compte tenu de la prise de conscience des acteurs.

Avant de s’attarder sur la méthodologie de recherche employée à travers cette étude, tentons de définir les origines de la cybersécurité et les enjeux qui, aujourd’hui, ont fait de cette discipline l’une des plus grandes préoccupations des entreprises et institutions partout dans le monde.

**Méthodologie de recherche**

Nous souhaitons comprendre si les évènements liés aux failles de sécurité dans les systèmes d’information peuvent avoir un impact assez important pour causer des pertes financières significatives et ainsi dévaluer les actions des entreprises cotées en France. Aussi, nous allons procéder à une méthode d’analyse et de sélection d’échantillons largement démontrée dans des études antérieures : l’étude d’évènements (Campbell, 2003 ; Gordon, 2011 ; Arcuri, 2017 ; Peillex et Ureche-Rangau, 2014 ; Peillex et Ureche-Rangau, 2015 ; El Ouadghiri et al., 2016 ; Peillex, 2014 ; Jaballah et al., 2018 ; El Ouadghiri et Peillex, 2018 ; El Ouadghiri et al., 2019 ; Peillex et al., 2021).

L’étude d'évènements permet de mesurer l'impact des atteintes à la sécurité des systèmes d’information sur les rendements des actions. L'hypothèse repose sur le fait que les marchés financiers réagissent aux annonces affectant la valeur d'un titre, de sorte que les rendements boursiers sont en mesure de saisir les coûts implicites et explicites des cyberattaques (Arcuri, 2017 ; Acquisti, 2006). En particulier, si une entreprise souffre d'une atteinte à la sécurité de son système d’information, elle peut subir des pertes financières qui devraient se refléter sur son cours boursier. Les cotations en bourse qui entourent l'évènement peuvent capter l'impact de cette annonce et mesurer le coût économique de la cyberattaque. La méthodologie de l'étude d'évènements est basée sur l'hypothèse de l’efficience des marchés développée par Fama et soutenant que le prix d’un actif sur un marché liquide et efficient reflétera en tout temps toute l’information disponible. Par conséquent, il sera impossible de tirer un rendement « anormal » de ce titre compte tenu de son risque (Fama, 1969).

En 1969, Fama, Fisher, Jensen et Roll (Fama et coll., 1969) ont publié dans « International Economics Review » leur méthodologie appelée depuis « event study methodology ». Cette méthodologie s’appuie sur les résultats des cours boursiers afin d’expliquer les effets qui peuvent apparaître à la suite d’un évènement rendu public. Dans leur démarche, ils ont étudié l’impact produit par l’annonce d’opération de division d’actions sur les actionnaires, aussi appelé « Stock split » (Boufama, 2013). Dans cette optique, ils exploitent le modèle de marché et le MEDAF afin de créer une relation linéaire entre la rentabilité du titre et la rentabilité du marché. Ce modèle est basé sur une approche statistique qui met en relation la rentabilité d’un titre avec le rendement de l’ensemble du marché. (Sharpe, 1963). Les rentabilités sont mesurées en différences logarithmiques (Peillex et Ureche-Rangau, 2014 ; El Ouadghiri et al., 2016 ; Erragragui et al., 2018 ; Benlemlih, et al. 2018).

L’objectif est d’examiner les réactions, suite aux annonces d’information d’une faille de sécurité dans les systèmes d’information, des cours boursiers. Pour ce faire plusieurs éléments doivent être définis, notamment la nature de l’échantillon, les paramètres d’analyse et le modèle permettant d’appréhender les rendements anormaux ou non des différents titres.

Les évènements qui composent l’échantillon doivent permettre de définir de manière exacte la date à laquelle ils ont eu lieu. Cette dernière est le point de départ de l’analyse utilisée dans cette étude et permettra d’établir une ligne temporelle. Cette ligne comprend la date de l’évènement ainsi que plusieurs fenêtres d’analyses qui l’entourent. Les périodes peuvent être antérieures et postérieures à la période d’évènement.

Dans le cadre de cette étude, la période d’évènement sera de 20 jours avant et 20 jours après l’attaque. Les fenêtres d’analyses étudiées dans cette étude reprennent la démarche utilisée en 2017 par Arcuri. (Arcuri et coll., 2017) En effet, aujourd’hui toutes les entreprises sont au fait des menaces cyber qui pèsent sur elles et les grandes entreprises ciblées dans cette étude font preuve d’une certaine maturité face à ce risque. Elles disposent de plans de gestion crises pour y faire face ainsi que de tout le support technique adéquat pour détecter et traiter ces menaces en quelques heures, au maximum jours. Les périodes entourant l’évènement supérieures à celle donnée précédemment ne semblent donc plus être aussi significatives qu’auparavant. De plus, la majorité des études citées précédemment ont tout de même démontré des résultats assez significatifs sur une période de 2 jours après l’annonce d’évènement.

Enfin, la période d’estimation, à l’extérieur de la période d’évènement, permet d’exclure l’effet de cette dernière. Elle sert de période de référence pour l’estimation des paramètres du modèle de marché. Comme de nombreuses études ayant suivies la même méthodologie d’étude d’évènement, cette période a été fixée à 121 jours (Skrepnek et coll., 2001). Ainsi, les coefficients αi et βi sont estimés pour chaque entreprise à l’aide d’une régression de 𝑅𝑖 sur 𝑅𝑚𝑡 pour une période d’estimation de 100 jours (du 21 au 121e jour avant l’annonce de la cyberattaque, compte tenu de notre période d’évènement de 20 jours).

## Collecte des données

Les données collectées se fondent sur la littérature académique, sur les rapports de l’industrie, ainsi que sur différentes interviews et articles disponibles sur les moteurs de recherches. Les données quantitatives de cette étude sont collectées à partir du moteur de recherche Google et d’une base de données de journaux numériques. La recherche d’évènements s’appuie également sur la base de données de la communauté VCDB VERIS, contenant des milliers d’incidents documentés et issus d’entreprises publiques partout dans le monde. Un dernier outil a aidé à la collecte de données de cette étude, la communauté ZATAZ. C’est avant tout un site web français qui a pour vocation la vulgarisation de l’information et de la délinquance informatique. Il est notamment reconnu pour son protocole d’alerte qui vise à alerter l’entreprise et les autorités compétentes lorsqu’une faille informatique est détectée. Ainsi, beaucoup d’évènements ayant eu lieu en France ces dernières années sont notifiés au travers de ce site internet.

L’essentiel des incidents relevés sont issus de recherches à partir des mots clés suivants : « attaque par déni de service », « bourse de Paris », « cyberattaque », « cybermenace », « CAC 40 », « faille informatique », « faille de sécurité », « France », « hacker », « hameçonnage », « phishing », « rançongiciel », « ransomware », « système d’information », « sécurité, virus informatique » accompagné de noms d’entreprises et de dates clés.

L’objectif est de collecter les données relatives aux cyberattaques ayant été déclarées entre 2009 et 2019 soit un périmètre de dix années. Les évènements identifiés devront respecter les critères suivants :

* L’entreprise est cotée sur le marché boursier français ;
* L’entreprise est cotée en priorité sur le CAC 40 et SBF 120 ;
* L’attaque a porté atteinte aux systèmes d’information d’une entreprise entre 2009 et 2019.

Contrairement aux différentes études précédemment citées, nous prendrons en considération dans notre échantillon les attaques produites à la fois au niveau des sociétés mères et celles produites au niveau des filiales. Cet échantillon complet d’attaques permet d’examiner toutes les conséquences des évènements liés à la cybersécurité. Afin d’obtenir un niveau d’analyse suffisant pour répondre aux hypothèses formulées précédemment plusieurs autres éléments devront être collectés. Les évènements de l’échantillon pourront être classés :

* par nom d’entreprise ayant fait l’objet de faille de sécurité pendant la période définie ;
* par lieu de cotation ;
* par taille de capitalisation boursière ;
* par secteur d’activité ;
* par type d’atteinte à la sécurité subie ;
* par intensité d’attaque subie.

Ces critères permettront de segmenter l’analyse de cette étude et trouver des facteurs de corrélation avec l’hypothèse principale d’identification d’un rendement anormal suite à l’annonce publique d’une faille de sécurité. Enfin, une fois l’échantillon constitué et notre base de données fiabilisée, les cours des actions ont été collectés via la base de données financière Bloomberg.

**Résultats et analyses**

L’échantillon présenté dans cette étude est constitué de 53 incidents de sécurité informatique tous contenus dans les critères précédemment définis. Ces 53 incidents ont donné lieu à des incidents dans 35 entreprises côtés sur le marché du CAC 40 et SBF 120. Elles ont été réparties dans 18 secteurs d’activités différents.

Le tableau 1, reprend la répartition des événements étudiés en fonction du secteur d’activité dans lequel évolue l’entreprise concernée.

Assez rapidement on s’aperçoit que près de 19% des attaques collectées ont eu lieu dans des établissements bancaires ou d’assurances. Ces entreprises détiennent des données personnelles à fortes valeurs ajoutées, notamment les données bancaires des clients de ces établissements.

Le tableau 2, permet de mettre en évidence la répartition des évènements étudiés en fonction de l’année de survenance. On remarque, à première vue, que 57% des attaques collectées sont survenues ces deux dernières années. Ces éléments d’observations permettront de mettre en avant certains phénomènes et aideront à la validation ou non des hypothèses formalisées dans cette étude.

Tableau 1 : Distribution des événements par secteur d’activité

|  |  |
| --- | --- |
| **Secteur d'activité** | **Nombre d’attaques** |
| Banque / Assurance | 10 |
| Audiovisuel et divertissements | 6 |
| Aérospatiale | 5 |
| Télécommunications filaires | 5 |
| Services | 4 |
| Distributeur | 3 |
| Énergie | 3 |
| Alimentation | 2 |
| Automobiles | 2 |
| Construction | 2 |
| Hôtellerie | 2 |
| Santé | 2 |
| Sociétés pétrolières et gazières intégrées | 2 |
| Agro-alimentaire | 1 |
| Compagnies aériennes | 1 |
| Eau | 1 |
| Matériaux et accessoires de construction | 1 |
| Promotion immobilière | 1 |
| **Total général** | **53** |

Tableau 2 : Distribution des évènements par année de survenance

|  |  |
| --- | --- |
| **Année de survenance** | **Nombre d'attaques** |
| 2019 | 18 |
| 2018 | 12 |
| 2017 | 9 |
| 2016 | 4 |
| 2015 | 3 |
| 2014 | 4 |
| 2013 | 2 |
| 2011 | 1 |
| **Total général** | **53** |

Ce tableau 3 présente la répartition chronologique des 53 cyberattaques réussies au cours de la période allant de 2011 à 2019. Les pourcentages de cyberattaques survenues pendant chacune des années et pour chaque industrie au cours de la période de référence sont inscrits en italique. Il permet de mieux visualiser les données fournies dans les tableaux 1 et 2 et confirme ainsi que le secteur le plus touché est celui des banques et assurances (19%) probablement dû au fait qu’ils collectent beaucoup de données sur une très large population de clients.

Tableau 3 : Distribution des cyberattaques par an et par industrie

**Aérospatiale**

**Alimentation**

**Audiovisuel et**

**divertissements Automobiles**

**Compagnies aériennes**

**Construction**

**Distributeur**

**Energie**

**Santé**

**Service**

**Télécommunications filaires**

**Banque / Assurance**

**Total général**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2019 | 4 | 1 | 2 |  |  |  | 1 | 2 | 2 | 1 | 1 |  | 4 | **18** | *34%* |
| 2018 |  | 1 | 1 |  | 1 |  | 1 |  |  |  | 4 | 1 | 3 | **12** | *23%* |
| 2017 |  |  | 1 | 1 |  |  | 1 | 1 | 1 |  | 1 | 1 | 2 | **9** | *17%* |
| 2016 |  |  | 1 |  |  |  | 1 |  |  | 1 |  | 1 |  | **4** | *8%* |
| 2015 |  | 1 | 1 |  |  |  |  |  | 1 |  |  |  |  | **3** | *6%* |
| 2014 | 1 |  |  |  |  |  |  |  |  |  |  | 2 | 1 | **4** | *8%* |
| 2013 |  |  |  | 1 |  |  |  |  | 1 |  |  |  |  | **2** | *4%* |
| 2011 |  |  |  |  |  |  |  |  | 1 |  |  |  |  | **1** | *2%* |
| **Total** | **5** | **3** | **6** | **2** | **1** |  | **4** | **3** | **6** | **2** | **6** | **5** | **10** | **53** |  |
| **général** | *9%* | *6%* | *11%* | *4%* |  | *2%* | *8%* | *6%* | *11%* | *4%* | *11%* | *9%* | *19%* |  |

**Analyse totale de l’échantillon**

La première analyse porte sur l’hypothèse selon laquelle, il existe une corrélation entre l’annonce d’une faille de sécurité et le rendement anormalement négatif des actions de notre échantillon. Huit fenêtres d’analyse ont été constituées. La moitié d’entre elles sont des fenêtres qui encadrent le jour de l’annonce (t =0) à quelques jours près, soit [0 ; 1], [0 ; 3], [-1 ; 1] et [-1 ; 3]. Ces fenêtres sont les plus intéressantes à étudier puisqu’aujourd’hui, 55% des entreprises affirment avoir contrôlé l’attaque dans les 24h alors que 88% d’entre elles sont détectées en moins d’une journée. (Accenture, 2020) Quatre autres fenêtres, plus larges autour de l’évènement ont également été étudiées afin de mesurer l’impact de l’annonce sur le moyen terme. Ces fenêtres sont : [-1 ; 5], [ - 1 ; 10], [-1 ; 15] et [-1 ; 20].

Pour la fenêtre [0 ; 1], la moyenne des rendements cumulés moyens est de – 0,0068 pour l’ensemble des entreprises de l’échantillon. Ce chiffre indique qu’entre le jour de l’annonce de la faille de sécurité et le jour suivant l’annonce, le portefeuille des entreprises a diminué de 0,68% par rapport à leur valorisation boursière initiale. Cependant la valeur ne semble pas significative au seuil de 5%. Ce qui signifie qu’on ne peut pas affirmer qu’une différence significative existe entre la moyenne anormale estimée et la moyenne observée sur le marché.

Sur la fenêtre [-1 ;1], on constate que le RACM est de – 0,0005 et donc moins important que sur la fenêtre précédente. Cette analyse nous permet de supposer que les annonces ne sont pas anticipées par les actionnaires et plus globalement par le marché. Le retour anormal sur cette fenêtre est relativement faible et proche de 0%. En comparaison avec d’autres études qui ont étudié cette même fenêtre d’événement, notre résultat est plutôt cohérent bien qu’un peu plus faible (Kamiya et coll. (2020) – RACM [-1 ;1] - 0,0084).

Globalement on peut observer des rendements anormaux sur les périodes proches de l’évènement et pour la majorité des entreprises (68% et 64% des entreprises de l’échantillon à très court terme).

Tableau 4 : Résultats d’analyse de la totalité de l’échantillon

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Fenêtre d’événement** | **Moyenne RAM** | **t-value** | **Médiane RAM** | **t-value** | **%****rendement négatif** |
| **[0;1]** | -0,0068 | -1,451 | -0,0090 | -4,135\*\*\* | 68% |
| **[0;3]** | -0,0068 | -1,446 | -0,0093 | -4,282\*\*\* | 58% |
| **[-1;1]** | -0,0005 | -0,107 | -0,0064 | -2,936\*\*\* | 64% |
| **[-1;3]** | -0,0005 | -0,102 | -0,0126 | -5,807\*\*\* | 62% |
| **[-1;5]** | 0,0071 | 1,518 | 0,0011 | 0,515 | 49% |
| **[-1;10]** | 0,0034 | 0,718 | 0,0057 | 2,607\*\* | 47% |
| **[-1;15]** | -0,0069 | -1,467 | -0,0147 | -6,782\*\*\* | 58% |
| **[-1;20]** | -0,0070 | -1,480 | -0,0090 | -4,138\*\*\* | 51% |

Ces premiers résultats permettent de valider la première hypothèse selon laquelle on observe un rendement anormal sur l’ensemble de l’échantillon, et ce sur plusieurs fenêtres sélectionnées. En majorité, l’échantillon est composé d’évènements ayant entrainé des rendements anormalement négatifs. Le test de student ne permet pas de valider ces observations au seuil de 5%. Cependant, l’étude repose sur un échantillon de 53 évènements ce qui peut expliquer le manque de significativité observé avec ce test statistique.

**Analyse par secteur d’activité**

Dans la description caractéristique de l’échantillon, nous avons pu observer que trois secteurs de notre échantillon sont plus touchés par les cyberattaques. Ces secteurs sont ceux qui disposent de données sensibles et à forte valeur ajoutée dans les domaines de la banque et assurance (19% des attaques collectées), de l’audiovisuel et du divertissement (11% des attaques collectées) et de l’aérospatial (9% des attaques collectées). Cette analyse va nous permettre de valider ou non la seconde hypothèse de cette étude selon laquelle, une atteinte à la sécurité des systèmes d’information d’une entreprise entraîne une rentabilité anormalement négative sur le rendement de ses actions lorsqu’elle est rendue publique en fonction de son secteur d’activité. Afin de pouvoir comparer les moyennes cumulées, les secteurs avec moins de cinq évènements ne sont pas analysés.

Tableau 5 : Résultats d’analyse de la RAMC par secteur d’activité

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Fenêtres****d’ évènements** | **Banque / Assurance** | **Audiovisuel et divertissements** | **Énergie** | **Service** | **Aérospatiale** | **Télécommunications filaires** |
| *Nombre**d’évènements* | *10* | *6* | *6* | *6* | *5* | *5* |
| **[0;1]** | -0,0054 | 0,0016 | -0,0090 | 0,0018 | -0,0056 | 0,0027 |
| *t-value* | *-1,1401* | *0,3494* | *-1,9159* | *0,3870* | *-1,1795* | *0,5786* |
| **[-1;1]** | -0,0056 | 0,0380 | -0,0145 | 0,0110 | 0,0007 | 0,0005 |
| *t-value* | *-1,185* | *8,079* | *-3,080* | *2,346* | *0,148* | *0,098* |
| **[0;3]** | -0,0033 | -0,0101 | -0,0151 | 0,0101 | -0,0195 | 0,0006 |
| *t-value* | *-0,6990* | *-2,1355* | *-3,2147* | *2,1445* | *-4,1418* | *0,1292* |
| **[-1;5]** | -0,0204 | 0,0487 | -0,0144 | 0,0325 | -0,0087 | -0,0009 |
| *t-value* | *-4,3421* | *10,3520* | *-3,0527* | *6,8971* | *-1,8512* | *-0,2011* |

Au travers les résultats d’analyse de la RAMC par secteur d’activité on observe que certains domaines ne semblent pas être sensibles aux annonces de faille de sécurité. C’est le cas des sociétés de services qui n’observent en moyenne sur les quatre fenêtres d’évènements sélectionnées, aucun rendement négatif moyen. Les secteurs de la télécom et de l’audiovisuel semblent également très peu sensibles aux annonces. En revanche, les établissements bancaires et assurances observent des RAMC sur l’ensemble des périodes observées. Sur la fenêtre [-1 ;5] ce secteur observe un rendement négatif de 2,04% avec un niveau de significativité important. Il est donc très probable qu’une entreprise de ce secteur, si elle subit une attaque portant atteinte à ses systèmes d’information, observe des rendements négatifs anormaux du même ordre. Le secteur de l’énergie semble également subir des rendements anormalement négatifs dans les jours qui entourent et suivent l’annonce d’une faille de sécurité informatique. Sur l’ensemble des fenêtres observées, le RAMC varie de -0,9% à -1,51% avec des niveaux de significativités tous satisfaisant au moins au seuil de 5%.

Ces deux secteurs ont donc l’air de subir des pertes plus importantes sur leur valorisation boursière que d’autres. Ce sont deux secteurs essentiels dans le bon fonctionnement de la vie de français. Nombre des entreprises de ces secteurs sont notamment qualifiées d’OIV et doivent ainsi démontrer un niveau de sécurité sur leurs systèmes d’information plus importants. Une atteinte à ces systèmes peut donc être perçue beaucoup plus négativement par les investisseurs et actionnaires. Les coûts directs et indirects engendrés par ces attaques peuvent avoir des impacts bien plus significatifs. Enfin, ces deux secteurs manipulent des données à forte valeur ajoutée. Ils disposent d’immenses bases de données clients avec des informations importantes comme des coordonnées bancaires, des numéros de téléphone, d’adresse mails... Ce sont des données particulièrement recherchées par des hackers puisqu’ils pourront par la suite détourner l’usage initial de ces données et notamment passer des ordres de virement et les valider.

L’hypothèse 2 selon laquelle une atteinte à la sécurité des systèmes d’information d’une entreprise entraîne une rentabilité anormalement négative sur le rendement de ses actions lorsqu’elle est rendue publique en fonction de son secteur d’activité semble être validée. Bien que certains secteurs semblent accuser des rendements plus négatifs que d’autres, on peut se demander si cet écart n’est pas plutôt lié au type de cyberattaque ayant porté atteinte à l’entreprise concernée.

**Analyse par type de cyberattaque**

Aujourd’hui, l’ingénierie sociale, théorisée en 2002 par Kevin Mitnick est l’attaque la plus courante. Cette pratique consiste à utiliser les failles humaines comme effet de levier pour atteindre les systèmes d’information des entreprises. C’est notamment ce sur quoi repose le phishing ou hameçonnage en français, représentant le premier type de cyberattaque en France et dans le monde. (Accenture, 2019) Les malwares et ransomwares font également partie des attaques les plus rependues suivies par les DDOS et attaques de type injection SQL et celles de l’Homme au milieu. Cependant, les attaques les plus coûteuses sont celles qui concernent des fraudes internes avant les injections de code malveillant et les DDOS.(Accenture, 2019)

Sur la fenêtre d’évènement [0 ; 1], l’attaque Man in the middle (MIMA), ou l’homme au milieu et Drive by Downloald22 sont celles pour lesquelles les rendements anormalement négatifs sont les plus importants avec 4,17% et 1,21%. La méthode Drive by Download est particulièrement redoutable puisqu’elle s’exécute automatiquement. Le seul moyen d’y faire face est d’être en possession de logiciels antivirus et pare feu performants et bien configurés afin de bloquer à temps les téléchargements. Sur les attaques de type ingénierie sociale, on observe des rendements anormalement négatifs sur l’ensemble des fenêtres d’évènements cependant aucun d’entre eux n’excède 1%. Comme le confirme l’étude Accenture sur le coût des cyberattaques, bien que très répandues, ces attaques ne semblent pas être les plus coûteuses. En effet, généralement ces attaques sont détectées très rapidement puisqu’elles sont d’origine humaine. Cependant, le phishing est bien souvent le moyen d’atteindre les systèmes d’information discrètement afin de s’y déplacer, extraire et crypter des données petit à petit pendant plusieurs semaines ou espionner les collaborateurs. Dans un second temps, les hackers installent un malware directement sur les SI des entreprises visant à les rendre inopérants et réclament une rançon en échange de la clé de déchiffrement. Dans ce cas l’attaque initiale n’a plus du tout le même impact sur l’entreprise que ce soit d’un point de vue image ou business.

En effet, on remarque que les ransomwares entraînement des rendements anormalement négatifs plus importants que le phishing en lui-même sur les fenêtres [0 ;3] et [-1 ; 5] avec des seuils de significativité satisfaisants. Sur les deux autres fenêtres, beaucoup plus proches de l’annonce, les effets sont très faibles. En effet, sur les méthodes d’attaque avec les ransomwares, les entreprises mettent souvent plusieurs jours à réparer, restaurer les SI et retrouver un niveau opérationnel satisfaisant. En janvier 2020, le ransomware MAZE a porté atteinte aux SI de Bouygues Construction, une société de BTP du groupe Bouygues, côté sur le CAC 40. Une rançon de 10 millions d’euros a été demandée par le groupe de hackers. Deux mois plus tard, Bouygues admet ne pas avoir encore pu rétablir totalement la situation. Les équipes IT mettent donc plusieurs jours à évaluer l’ampleur de ce type d’attaque d’ampleur.

Tableau 6 : Résultats d’analyse de la RAMC par type d’attaque

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Fenêtre d'évènement** | **DDOS** | **Faille de sécurité** | **Malware** | **Phishing** | **Ransomware** | **SQL injection** | **Drive by****Download** | **MIMA** |
| *Répartition* | *8%* | *15%* | *25%* | *19%* | *19%* | *4%* | *4%* | *8%* |
| **[0;1]** | -0,0010 | -0,0097 | -0,0088 | -0,0070 | 0,0018 | 0,0087 | -0,0417 | -0,0121 |
| *t-value* | *-0,2168* | *-2,0520* | *-1,8673* | *-1,4771* | *0,3748* | *1,8520* | *-8,8702* | *-2,5739* |
| **[0;3]** | 0,0013 | -0,0237 | -0,0044 | -0,0024 | 0,0117 | 0,0079 | -0,0466 | -0,0334 |
| *t-value* | *0,2719* | *-5,0359* | *-0,9439* | *-0,5175* | *2,4837* | *1,6762* | *-9,9063* | *-7,0891* |
| **[-1;1]** | -0,0105 | -0,0055 | -0,0125 | -0,0034 | 0,0049 | 0,0403 | -0,0323 | 0,0478 |
| *t-value* | *-2,2366* | *-1,1653* | *-2,6646* | *-0,7265* | *1,0411* | *8,5719* | *-6,8656* | *10,1666* |
| **[-1;5]** | -0,0130 | -0,0085 | 0,0019 | 0,0069 | 0,0198 | 0,0354 | -0,0081 | 0,0380 |
| *t-value* | *-2,7597* | *-1,8097* | *0,4094* | *1,4594* | *4,2166* | *7,5194* | *-1,7147* | *8,0726* |

L’hypothèse 3 selon laquelle une atteinte à la sécurité des systèmes d’information d’une entreprise entraîne une rentabilité anormalement négative de plus ou moins grande importance sur la valeur de ses actions lorsqu’elle est rendue publique en fonction du type d’atteinte aux systèmes d’information semble être validée. En effet, on observe des disparités entre les différentes méthodes d’attaques. De plus, ces disparités semblent être corrélées au coût direct et indirect de ces mêmes types d’attaques exposés dans d’autres études publiées récemment.

**Analyse par type de données compromises**

Nous avons pu voir que certains secteurs sont plus à même de subir des attaques entraînant des rendements anormalement négatifs. La méthode employée pour la cyber attaque a également une influence sur les rendements négatifs, cependant, le type de données touchées doit également avoir une influence. En effet, nous avons pu exposer, précédemment, dans cette étude que certaines données comme les données personnelles sont de plus en plus encadrées par les autorités compétentes comme la CNIL en France. Sous peine de manquement et de non-conformité notamment au RGPD, les entreprises européennes s’exposent à des amendes financières. On peut donc penser que des atteintes portées à ces données peuvent avoir un impact plus important en partie à cause du risque d’image qui pèse sur les entreprises assujetties. Les actionnaires dans la même logique peuvent prendre des positions plus sécurisantes à l’annonce de faille de sécurité sur ce type de données. Le vol de données corporate peut être également très dommageable pour les entreprises et d’autant plus si elles appartiennent à certains secteurs plus à risque.

À la lecture du Tableau 7, il apparaît clairement que les attaques n’ayant porté atteinte à aucune donnée n’entraînent pas de rendement négatif très important (inférieur à 0,6%).

En revanche, les données confidentielles, les données relatives aux entreprises, à leur fonctionnement, aux processus internes entraînent des rendements anormalement négatifs moyens toujours au moins supérieurs à 1,2% avec tests de significativité tous validés. Ces résultats confirment bien l’importance de ces données pour les entreprises et leurs actionnaires. C’est notamment le cas pour les entreprises qui évoluent sur des secteurs hyperconcurrentiels et dont l’accès au marché est compliqué. Ces entreprises se doivent de garder le moindre avantage compétitif dont elles disposent.

Enfin, on peut observer que les données personnelles restent visiblement les plus convoitées puisqu’elles sont concernées dans au moins 71% des attaques de l’échantillon de cette étude. Si on se focalise uniquement sur les cyberattaques ayant fait l’objet d’une atteinte aux données personnelles, les RAMC sont négatifs sur l’ensemble des fenêtres d’évènements, mais pas avec la même intensité. Sur les fenêtres [0 ; 1] et [0 ; 3], on peut constater que les rendements négatifs, respectivement 1,06% et 1,24%, sont du même ordre que ceux des données confidentielles. Les tests de student de significativité viennent appuyer ces statistiques sur ces deux fenêtres. En revanche, sur les fenêtres [-1 ; 1] et [-1 ;5] on constate des rendements anormaux très proches de 0%. On peut alors supposer que ces fenêtres à -1 jour anticipent trop la perte de valeur du cours de bourse et que les pertes engendrées par les données personnelles ne peuvent être anticipées. De plus, on découvre souvent que quelques heures, ou jours après l’attaque, le nombre exact et le type de données compromises.

Les données classées secret défense, données présentant un caractère de secret de la Défense nationale dont la diffusion et l’accès est très restreint sont peu atteintes et donc visiblement bien protégées. Cependant lorsqu’elles sont touchées, les impacts pour les rendements boursiers sont très forts. On constate alors des RAMC négatifs pour l’ensemble des fenêtres d’évènement entre 3,91% et 5,55%.

Tableau 7 : Résultats d’analyse de la RAMC par type de données touchées

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Fenêtre d'évènement** | **Aucune perte de données** | **Données confidentielles** | **Données personnelles** | **Données personnelles et confidentielles** | **Secret défense** |
| *Répartition* | *13%* | *13%* | *60%* | *11%* | *2%* |
| **[0;1]** | 0,0018 | -0,0127 | -0,0106 | 0,0024 | 0,0391 |
| *t-value* | *0,3847* | *-2,6997* | *-2,2526* | *0,5113* | *5,6435* |
| **[0;3]** | -0,0060 | -0,0165 | -0,0124 | 0,0241 | 0,0474 |
| *t-value* | *-1,2846* | *-3,4952* | *-2,6257* | *5,1292* | *6,4885* |
| **[- 1;1]** | -0,0032 | -0,0194 | 0,0005 | 0,0120 | 0,0440 |
| *t-value* | *-0,6882* | *-4,1113* | *0,1033* | *2,5441* | *6,3462* |
| **[-1;5]** | 0,0059 | -0,0173 | 0,0038 | 0,0470 | 0,0555 |
| *t-value* | *1,2522* | *-3,6860* | *0,8053* | *9,9885* | *8,0181* |

L’hypothèse 4 selon laquelle une atteinte à la sécurité des systèmes d’information d’une entreprise entraîne une rentabilité anormalement négative de la valeur de ses actions lorsqu’elle est rendue publique en fonction du type de données touchées ou ciblées est vérifiée. On a pu observer que lorsque les données ne sont pas atteintes les rendements restent cohérents avec les tendances observées sur la période. En revanche, si des données sont atteintes des comportements différents sont constatés et peuvent être expliqués par plusieurs facteurs, dont le volume de données, ou leur niveau de confidentialité.

**Analyse de l’évolution de l’impact des cyberattaques dans le temps**

Globalement, jusqu’à présent nous avons pu valider l’ensemble des hypothèses à plusieurs degrés. Un très grand nombre d’observations ont démontré des RAMC négatifs selon différents critères et sur plusieurs fenêtres d’évènements. Notre dernière analyse cherche à démontrer si les cyberattaques entraînent des RAMC différents ces deux dernières années que les années précédentes. On a pu développer précédemment dans cette étude la prise de conscience de tous les acteurs quant au risque cyber, à ses coûts et mesures pour les minimiser dans toutes les entreprises et institutions françaises et européennes.

À la lecture de ce dernier tableau d’analyse, on observe que sur les fenêtres très proches de l’annonce [0 ;1] et [-1 ; 1], les RAMC sont plus négatifs sur les évènements de notre échantillon sur la période allant de 2011 à 2017. Au contraire, sur les mêmes fenêtres observées, les attaques ayant eu lieu en 2018 et 2019 accusent des RAMC négatifs plus faibles voir très faible pour 2019 (0,48% et 0,31%).

Sur les fenêtres d’une durée supérieure à 5 jours, les RAMC des annonces de cyberattaques sur la période 2011 à 2017 deviennent alors anormalement positifs.

Sur 2018 et plus particulièrement sur 2019, on observe des RAMC négatifs plus importants sur des fenêtres plus longues et supérieures à +1 jour suite à l’annonce de faille de sécurité. Cependant, les RAMC négatifs sont relativement faibles sur l’année 2019 alors que le nombre de cyberattaques ne cesse d’augmenter chaque année en France.

Tableau 8 : Résultats d’analyse d’évolution de la RAMC dans le temps

|  |  |  |  |
| --- | --- | --- | --- |
| **Fenêtre d'évènement** | **2011 - 2017** | **2018** | **2019** |
| *Nombre de Type d'attaque* | *43,40%* | *22,64%* | *33,96%* |
| [0;1] | -0,0114 | -0,0108 | -0,0048 |
| t-value | -2,4325 | -2,2957 | -1,0163 |
| [0;3] | -0,0083 | -0,0185 | 0,0003 |
| t-value | -1,7683 | -3,9272 | 0,0650 |
| [-1;1] | -0,0109 | -0,0026 | -0,0031 |
| t-value | -2,3175 | -0,5582 | -0,6502 |
| [-1;5] | 0,0066 | -0,0081 | 0,0073 |
| t-value | 1,4047 | -1,7171 | 1,5486 |
| [-1;10] | 0,0037 | -0,0108 | 0,0050 |
| t-value | 0,7756 | -2,2914 | 1,0618 |

L’hypothèse 5 selon laquelle une atteinte à la sécurité des systèmes d’information d’une entreprise entraîne une rentabilité anormalement négative si elle a eu lieu ces deux dernières années compte tenu de la prise de conscience des acteurs n’est pas réellement vérifiée. En effet, c’est plutôt l’effet contraire qui est constaté. On peut alors supposer que les exigences réglementaires qui pèsent sur les entreprises se révèlent efficaces. Les établissements cotés ont saisi les enjeux et investi massivement dans des programmes et outils pour réduire le risque inhérent au cyberespace. On peut également penser qu’avec les années et l’expérience des précédentes cyberattaques subies, les actionnaires sont moins sensibles à ces annonces de faille de sécurité. En effet, aujourd’hui nous sommes tous concernés par ce risque cyber devenu systémique, les marchés réagissent peut-être moins intensément. Les réactions observées sur les marchés ne retranscrivent pas, dans ce cas précis, la tendance observée dans les entreprises sur les coûts des cyberattaques. Sur ces deux dernières années, le coût des cyberattaques a augmenté d’environ 12% chaque année (Accenture, 2019) et devrait augmenter de 72% dans les cinq années à venir.

# Conclusion

L’impact d’une annonce de faille de sécurité informatique sur la rentabilité d’un portefeuille d’action est un sujet qui a intéressé beaucoup de chercheurs depuis la fin des années 1990. Les premières études ne parvenaient pas à aboutir à une affirmation claire et étaient centrées sur des évènements impactant les entreprises américaines. Avec le temps, les études se sont diversifiées et complexifiées prenant en compte de plus en plus de facteurs propres à l’informatique comme le type de cyberattaque. Avec la mondialisation et l’expansion des réseaux informatiques et télécom, l’hyper connectivité et le développement de l’internet des objets, des études ont pu être menées sur des populations plus diverses. Aujourd’hui, notre étude s’est focalisée sur les entreprises du marché boursier français, car peu d’études se sont attardées à analyser uniquement cette population.

À travers notre travail empirique, nous avons cherché à démontrer dans quelle mesure l’annonce d’une faille informatique, d’une cyberattaque pouvait influencer la rentabilité des cours boursiers. L’une des difficultés majeures de cette étude a été de collecter des données pertinentes et de qualité. En effet, les cyberattaques entraînent des coûts pour les entreprises et il n’est jamais très bien perçu de subir une attaque de ce type. Les obligations de déclarations sont très récentes et ne concernent que certains types de données compromises. Ainsi, beaucoup de cyberattaques sont laissées en silence, traitées en interne dans la plus grande discrétion. Le portefeuille d’évènement du travail empirique fait tout de même état de 53 attaques. Ce chiffre peut être jugé satisfaisant pour la réalisation d’un travail de recherche, d’autant que des précédents travaux sur la même thématique ont précédemment été menés avec de plus petits échantillons. Cependant, cela reste assez faible pour une étude d’évènement et a probablement pu créer certains biais notamment dans l’estimation des rendements anormaux.

L’hypothèse principale de l’étude selon laquelle une atteinte à la sécurité des systèmes d’information d’une entreprise entraîne une rentabilité anormalement négative de la valeur de ses actions lorsqu’elle est rendue publique est validée. En effet, on a pu constater des rendements négatifs sur les deux tiers des fenêtres analysées. Les rendements positifs sont constatés sur les fenêtres de plus de 6 jours et avec des anticipations à J -3 et J-5. Ces résultats ont permis d’affirmer que les marchés ne peuvent pas anticiper les cyberattaques ni leurs annonces et que l’impact négatif est généralement absorbé sous 3 à 5 jours. Globalement, les quatre autres hypothèses plus spécifiques ont été également validées avec des niveaux différents. Les résultats sont cohérents au vu des études actuelles notamment sur les tendances des cyberattaques, les méthodes et impacts ces dernières années.

Selon les résultats établis dans l’hypothèse 5, il apparaît qu’en 2019, les rendements ont été un peu moins négativement impactés que les années précédentes. Cette dernière statistique est intéressante, car assez contradictoire avec les tendances de ces dernières années. En effet, on a pu lire précédemment dans l’étude que les coûts des cyberattaques ne cessent d’augmenter et devraient augmenter de 72% dans les cinq années à venir. Face à l’hostilité du cyberespace et la nécessité de prendre part aux différentes transitions numériques, les entreprises ont renforcé la sécurité de leurs systèmes d’information. Ce mouvement est très fortement encouragé par la législation française et européenne mise en place à l’égard du numérique et accompagnée par une stratégie globale de l’État. Les entreprises françaises ont intégré le risque cyber à leur approche globale par les risques, ainsi qu’à leurs cartographies des risques. Des méthodes d’analyse plus spécifiques au risque cyber sont également utilisées et visent à mieux connaître ses systèmes d’information, les menaces auxquels ils sont exposés afin de mieux se protéger, anticiper et répondre aux attaques. Des outils techniques sont déployés pour faire face aux vulnérabilités des SI et les minimiser. Ces solutions peuvent être très largement utilisées, c’est le cas des passerelles de sécurité mail (85%), des passerelles VPN/SSL (85%), et des proxy (83%) qui figurent parmi les solutions les plus mises en place. (CESIN, 2020) D’autres solutions peuvent s’avérer efficaces, particulièrement dans la lutte pour la protection des données comme les systèmes de chiffrement (45%) ou dans l’analyse comportementale avec la mise en place d’EDR.

Malgré tous ces investissements, les entreprises font face à de plus en plus d’attaques et doivent répondre aux menaces. La question n’est alors plus de savoir si une entreprise va se faire attaquer, mais plutôt se préparer à y faire face et minimiser les impacts opérationnels et financiers. Elles passent alors d’une dimension de cybersécurité à une dimension plus large qu’est la cyber résilience. Le National Institute of Standards and Technology (NIST) définit la cyber résilience comme la capacité à concevoir et à développer des systèmes capables d’anticiper, de résister, de se rétablir et de s’adapter à des conditions défavorables, à des contraintes, à des attaques utilisant des ressources cyber. Par cette approche, l’ensemble de l’entreprise est concerné à tous les niveaux hiérarchiques. Des scénarios de risques sont établis, adaptés aux contraintes de l’entreprise et testés à plusieurs échelles afin de simuler la réaction des acteurs, des infrastructures physiques et informatiques. On parle alors de plan de continuité d’activité et plan de secours informatique. Ces documents décrivent les stratégies à mettre en place en cas d’incident pour maintenir un niveau acceptable des activités vitales au bon fonctionnement de l’entreprise. Régulièrement des exercices, notamment de crises cyber, sont simulés afin de préparer au mieux les acteurs concernés à la gestion de crise en situation réelle.

Face à cette nouvelle approche, on remarque un changement marquant dans le management du risque depuis cinq ans. Les entreprises ont pris conscience de l’importance que prenaient les cyberattaques par ingénierie sociale comme le phishing. La cybersécurité n’est alors plus exclusivement réservée aux collaborateurs des services informatique mais concerne tous les membres de l’organisation. Afin de renforcer leur cyber résilience, les entreprises françaises mettent en place des programmes de sensibilisation à la cybersécurité. Ces programmes ont pour vocation de faire prendre conscience à tous les acteurs des risques et menaces que peuvent représenter leurs postes de travail, les outils informatiques. L’intérêt est également qu’ils se sentent partie intégrante de la stratégie de cybersécurité de l’entreprise et mesurent l’impact que peut avoir un simple clic, effectué des centaines de fois par jour sans s’en rendre forcément compte, sur l’ensemble de la société. Les programmes de sensibilisations peuvent prendre plusieurs formes, ils se veulent souvent ludiques (e-learning, business game, faux phishing) pour adresser un maximum de collaborateurs. Ainsi, aujourd’hui, 74% des entreprises françaises estiment que leurs salariés sont sensibilisés au risque cyber, et 55% pensent qu’ils respectent les recommandations. On peut constater que du travail reste à fournir sur cet aspect de sensibilisation cependant les programmes mis en place sont coûteux et les entreprises ont du mal à mesurer le retour sur investissement pour le moment. Des procédures sont mises en place pour tester le niveau de maturité des salariés et fournir un reporting pertinent aux membres de comité exécutif. Récemment, on voit apparaitre la notion de cybersécurité et la mise en place de programmes de sensibilisation dans les rapports annuels extra financiers des entreprises du CAC 40. La cybersécurité est alors considéré comme un enjeu stratégique pour la gouvernance des entreprises et leurs conseils d’administration. Elles sont tenues, au titre de la RSE de fournir des informations sur leurs données. L’évaluation qui en est faite devient alors un argument vis-à-vis des clients et des marchés financiers/investisseurs. Les actionnaires sont informés des mesures mises en place et peuvent apprécier le niveau de maturité de chaque entreprise en fonction de ce qui est évalué. Cependant, il n’existe pas aujourd’hui de référentiel harmonisé pour mesurer le niveau de maturité des entreprises françaises et de ses collaborateurs face au risque cyber. On pourrait se demander s’il n’est pas intéressant de créer un référentiel de reporting commun aux entreprises cotées sur le marché boursier français afin de fournir des indicateurs de performance pertinents aux investisseurs.

# Références

Accenture (2019). The cost of cybercrime. Annual cost of cybercrime study. Acquisti, A., et coll. (2006). Is there a cost to privacy breaches? An event study.

Amir, E. et coll (2018). Do Firms Underreport Information on Cyber-Attacks? Evidence from Capital Markets. SSRN Electronic Journal. 10.2139/ssrn.3136193.

Bener, A.B. (2000). Risk perception, trust and credibility: a case in Internet banking. University College of London, London.

Benlemlih, M., Jaballah, J., & Peillex, J. (2018). Does it really pay to do better? Exploring the financial effects of changes in CSR ratings. Applied Economics, 50(51), 5464-5482.

Benlemlih, M., & Peillex, J. (2019). Revisiter la question «Does it pay to be good?» dans le contexte européen. Recherches en Sciences de Gestion, (1), 243-263

Boufama, Omar. (2013). La méthodologie d'étude d'évènement : Une méthode et des outils à s'approprier en finance. Revue des sciences humaines.

Brockett, P.L. et coll. (2012). Enterprise cyber risk management. In: Risk management for the future – Theory and cases. Emblemsvag, J. (ed.), pp. 319-340

Campbell, K. et coll. (2003). The Economic Cost of Publicly Announced Information Security Breaches: Empirical evidence from the stock market, Journal of Computer Security 11(3): 431–448.

Cavusoglu, H et coll. (2004). The effect of Internet security breach announcements on market value: capital market reactions for breached firms and Internet security developers. International Journal of Electronic Commerce, 9(1), 69-104.

Desbrières, P., Erragragui, E., & Peillex, J. (2018). L’investissement conforme à la Charia est-il socialement responsable?. Management International/International Management/Gestión Internacional, 22(3), 51-64.

Desbrières, P., ERRAGRAGUI, E., & PEILLEX, J. (2017). L’investissement conforme à la Charia est-il socialement responsable?, Is Shariah compliant investment socially responsible? (No. 1171001). Université de Bourgogne-CREGO EA7317 Centre de recherches en gestion des organisations.

Ernst & Young (2018), EY Global Information Security Survey 2018–19.

El Ouadghiri, I., Mignon, V., & Boitout, N. (2016). On the impact of macroeconomic news surprises on Treasury-bond returns. Annals of Finance, 12(1), 29-53.

El Ouadghiri, I., & Peillex, J. (2018). Public attention to “Islamic terrorism” and stock market returns. Journal of Comparative Economics, 46(4), 936-946.

El Ouadghiri, I., & Uctum, R. (2016). Jumps in equilibrium prices and asymmetric news in foreign exchange markets. Economic Modelling, 54, 218-234.

El Ouadghiri, I., & Uctum, R. (2020). Macroeconomic expectations and time varying heterogeneity: evidence from individual survey data. Applied Economics, 52(23),2443-2459.

El Ouadghiri, I., Guesmi, K., Peillex, J., & Ziegler, A. (2019). Public attention to environmental issues and stock market returns (No. 22-2019). Joint Discussion Paper Series in Economics

Fama, E.F. (1970). Efficient Capital Markets: A review of theory and empirical work, Journal of Finance 25(2): 383–417.

Erragragui, E., Hassan, M. K., Peillex, J., & Khan, A. N. F. (2018). Does ethics improve stock market resilience in times of instability?. Economic Systems, 42(3), 450-469.

Fama, E.F. (1998). Market Efficiency, Long-term Returns, and Behavioral Finance, Journal of Financial Economics 49(3): 283–306.

Fama, Fisher et coll. (1969), The adjustment of stock prices to new information., International Economic Review, 10, pp. 1-21. In Journal of Research in Pharmaceutical Economics, vol 11, 2001, pp. 1-17.

Garg et coll. (2003). Quantifying the financial impact of IT security breaches. Inf. Manag. Comput.

Security. 11. 74-83.

Gordon, et coll. (2011). The impact of information security breaches: Has there been a downward shift in costs? , Journal of Computer Security, vol. 19, no. 1, pp. 33-56, 2011.

Hovav, A. and D’Arcy, J. (2003). The Impact of Denial-of-service Attack Announcements on the Market Value of Firms, Risk Management and Insurance Review 6(2): 97–121.

Hovav, A. and D’Arcy, J. (2004). The Impact of Virus Attack Announcements on the Market Value of Firms, Information Systems Security 13(3): 32–40.

Kamiya, et coll. (2018). What is the Impact of Successful Cyberattacks on Target Firms?. SSRN Electronic Journal.

Kamiya et coll. (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics. 10.1016/j.jfineco.2019.05.019.

Kannan, A. et coll. (2007). Market reaction to information security breach announcements: an empirical analysis. , International Journal of Electronic Commerce, 12(1), 69-91.

L’express.fr (2017), Cyberattaque mondiale "WannaCry", le ransomware qui chiffre les données.https://[www.lexpress.fr/actualite/monde/vague-internationale-de-](http://www.lexpress.fr/actualite/monde/vague-internationale-de-)cyberattaques\_1907798.html

Norton (2017), Norton Cyber Security Insights Report - Global Results

Peillex, J. (2014). L'Offre de produits de placement éthiques: décision de lancement, conception et réaction du marché financier (Doctoral dissertation, Amiens).

Peillex, J., Erragragui, E., Bitar, M., & Benlemlih, M. (2019). The contribution of market movements, asset allocation and active management to Islamic equity funds’ performance. The Quarterly Review of Economics and Finance, 74, 32-38.

Peillex, J., Boubaker, S., & Comyns, B. (2019). Does It Pay to Invest in Japanese Women? Evidence from the MSCI Japan Empowering Women Index. Journal of Business Ethics, 1-19.

Peillex, J., El Ouadghiri, I., Gomes, M., & Jaballah, J. Extreme heat and stock market activity. Ecological Economics, 179, 106810.

Peillex, J., & Comyns, B. (2020). Pourquoi les sociétés financières décident-elles d’adopter les Principes des Nations Unies pour l’Investissement Responsable?. Comptabilite-Controle-Audit, 26(1), 79-117.

Peillex, J., & Comyns, B. (2020). Why do financial companies adopt the United Nations Principles for Responsible Investment?. Comptabilité-Contrôle-Audit, 26(1), 79-117.

Peillex, J., & Ureche-Rangau, L. (2012). Création d'un indice boursier islamique sur la place financière de Paris: méthodologie et performance. Revue d'économie financière,(3), 289-314.

Peillex, J., & Ureche-Rangau, L. (2013). Is there a place for a shariah-compliant index on the Paris stock market?. International journal of business, 18(2), 131.

Peillex, J., & Ureche-Rangau, L. (2014). How does the Market Price of the Corporate Sponsor React to Socially Responsible Fund Introductions?. Bankers, Markets & Investors, (131), 17-29.

Peillex, J., & Ureche-Rangau, L. (2016). Identifying the determinants of the decision to create socially responsible funds: An empirical investigation. Journal of business ethics, 136(1), 101 117.

Peillex, J., & Ureche-Rangau, L. (2015). Comment expliquer la performance financière de l’investissement conforme à la Charia?. Management international/International Management/Gestiòn Internacional, 19(2), 128-139.

Shackelford S.J. (2012). Should Your Firm Invest in Cyber Risk Insurance?, Business Horizons, 55(4), 349-356.

Sharpe W. (1963), A simplified model for portfolio analysis , Management Science, pp. 277-293.

In Review of Quantitative Finance and Accounting, vol 11, 1998, pp. 111-137.

Skrepnek Grant & Lawson Kenneth, Measuring changes in capital market security: The event study methodology , Journal of Research in Pharmaceutical Economics, 11 (2001), pp. 1-17.

Winn, J. & Govern, K. (2009). Identity theft: risks and challenges to business of data compromise. Journal of Science Technology & Environmental Law, 28(1) , 49-63.

Ghernaouti-Hélie, Solange, Dufour Arnaud (2012), “Cybercriminalité et cybersécurité”, Presses Universitaires de France, « Que sais-je ? », p. 94-108

Ghernaouti, Solange, et Christian Aghroum (2012). “Cyber-résilience, risques et dépendances : pour une nouvelle approche de la cyber-sécurité”, Sécurité et stratégie, vol. 11, no. 4, pp. 74- 83.

IDC France, Blog (2019) <https://www.blog-idcfrance.com/>

Wavestone (2016) Opérateur d’importance vitale – Cybersécurité et conformité LPM https://[www.wavestone.com/app/uploads/2016/11/operateur-importance-vitale-cybersecurite-](http://www.wavestone.com/app/uploads/2016/11/operateur-importance-vitale-cybersecurite-) conformite-lpm.pdf