UCL Université catholique de Louvain

Faculté des sciences économiques, sociales, politiques et de communication (ESPO)
Ecole de communication (COMU)

Les stratégies communicationnelles des organisations lors de crises de cyberhacking

Mémoire réalisé par
Mégane Fastrez

Promoteur(s)
Damien Renard (promoteur)
Nicolas Vanderbiest (co-promoteur)

Année académique 2016-2017
Master en communication
Finalité spécialisée en gestion de la communication et des relations publiques

Table des matières

Introduction **2**

I. Définitions et contextualisation **4**
- **1. Qu'est-ce qu'une crise ?** **4**
- **2. De la criminalité à la cybercriminalité** **7**
- **3. Le cyberhacking, un type de crise** **8**
- **4. Le cycle de vie d'une crise** **10**
  - 1.1. Avant la crise 10
  - 1.2. Pendant la crise 11
  - 1.3. Après la crise 11
- **Le résumé du chapitre** **12**

II. La communication de crise **13**
- **1. Historique et définitions** **13**
- **2. Les théories en communication de crise** **14**
  - 2.1. Image Restoration Theory (W. Benoit) 15
  - 2.2. Situational Crisis Communication Theory (T. Coombs) 15
  - 2.3. Rhetorical Arena Theory (F. Frandsen & W. Johansen) 23
- **3. Les enjeux en communication de crise** **24**
  - 3.1. La gestion du temps 24
  - 3.2. La tonalité de la communication 24
  - 3.3. La cohérence des messages 25
- **Le résumé du chapitre** **26**

III. Approfondissement du concept de cyberhacking **27**
- **1. Typologie des crises de cyberhacking** **27**
- **2. Les modes opératoires d'un cyberhacking** **29**
- **Le résumé du chapitre** **34**

IV. Méthodologie et limites **35**
- **Le résumé du chapitre** **39**

V. Les stratégies communicationnelles lors de crises de cyberhacking ... **40**
  - 1.1. Le délai de communication 40
  - 1.2. Les canaux de communication 41
  - 1.3. Le choix de l'ambassadeur 42
  - 1.4. Les stratégies de réponse 42
- **Le résumé du chapitre** **46**

VI. Conclusion **47**
- **Le résumé du chapitre** **52**

Bibliographie **53**

Introduction

En mai 2017, une cyberattaque a fait « 200.000 victimes, essentiellement des entreprises, dans au moins 150 pays » selon le directeur d'Europol, Rob Wainright. Un logiciel malveillant a chiffré le contenu de certains ordinateurs pour rendre inaccessibles les données des propriétaires. Pour les récupérer, le hacker réclamait une rançon de 300 dollars. Des sites spécialisés tels que leakedsource.com[1] ou haveibeenpwned.com recensent des copies des données volées lors de piratages et sont généralement les premiers lanceurs d'alertes.

Ce type d'événement se produit régulièrement, au sein d'infrastructures de toutes tailles (des particuliers aux multinationales). **Avec l'émergence du big data, les organisations ont compris l'enjeu que représentent la récolte, le stockage et le traitement des données et l'ont intégré dans leur stratégie, mais les pirates informatiques aussi**. L'utilisation de ces données permet de renforcer le développement économique des organisations, mais ces informations sensibles sont souvent mal protégées.

Une crise impose une demande en communication qui dépasse ce à quoi l'organisation est habituée au cours de ses opérations quotidiennes (Frandsen et Johansen, 2017). **Ce mémoire a pour objectif d'identifier les pratiques et stratégies de communication mises en place par les organisations face à des crises de cyberhacking.** Les stratégies de réponses, les ambassadeurs, les canaux et délais de communication varient, mais les organisations font face à un dilemme moral vis-à-vis des parties prenantes : à qui la faute ?

Parmi les 102 organisations qui constituent mon échantillon d'analyse, pourquoi certaines ne communiquent que plusieurs mois après les événements ? Pourquoi la plupart d'entre elles n'assument-elles pas leurs responsabilités ? Quel(s) rôle(s) attribuent-elles aux différents canaux de communication en temps de crise ? Pourquoi certains profils d'ambassadeurs

[1] Ce site a été fermé par les autorités mais était encore accessible au début de la rédaction de ce mémoire

sont mis en avant dans certains secteurs, et moins dans d'autres ?

Dans le monde de la sécurité, un adage a été rendu célèbre par Robert Mueller (sixième du Bureau Fédéral d'Investigation) : « there are two types of companies, those that have been hacked, and those that don't yet know they have been hacked ». Si j'adaptais cet adage à l'observation faite dans ce mémoire qui traite de la communication de crise, il dirait : **il y a deux types d'organisations, celles qui ont communiqué sur leur piratage, et celles qui vont devoir le faire**.

I. Définitions et contextualisation

Avant même de commencer ma recherche, il fallait délimiter le sujet sur lequel j'allais travailler. Mon premier réflexe fut donc de récolter et reconstruire les définitions qui vont guider ma démarche. Parmi toutes les définitions du concept de « crise », laquelle correspond le mieux ? Qu'entendons-nous par « cyberhacking » ? Ces cas de cyberhacking peuvent-ils être considérés comme des crises ?

1. Qu'est-ce qu'une crise ?

« Toute étude sur les crises en vient à buter sur un problème de définition et de compréhension fondamentale : qu'entend-on par « crise » ? » (Lagadec, 1991, p. 44) car « elle est trop riche pour se laisser enfermer dans quelque proposition rédigée selon le principe de concision du dictionnaire » (Frandsen et Johansen, 2017, p. 34). Il ne s'agit pas exclusivement de ce domaine d'étude, dans de nombreuses disciplines les chercheurs se heurtent régulièrement au problème d'une définition statique de certains concepts. Les crises sont des processus complexes qui peuvent être examinés à différents niveaux et à partir de perspectives différentes en fonction du sujet de l'étude (Rosenthal et al., 2011b). C'est pourquoi, dans le cadre de ce mémoire il est d'autant plus nécessaire de délimiter ce concept de « crise » pour que chaque lecteur comprenne l'interprétation qui en sera faite.

La notion de crise est issue du terme grec « Krisis » qui signifie « décider », « faire un choix ». Actuellement, cette notion de crise est davantage utilisée pour caractériser la situation elle-même plutôt que l'action de décision. Au cours de l'Histoire, le mot crise s'est vu attribuer bon nombre de significations. Celles-ci relevaient à la fois du langage des tribunaux (discriminer), du langage médical (changement d'état voire pathologie), de la tragédie grecque (moments de vérité) et de la culture chinoise (opportunité). Même si une crise revêt un caractère principalement néfaste, je pense que prise au sérieux, elle peut surprendre de façon positive. Au final, à qui revient

le dernier mot en matière de définition d'une crise ? Qui va décider que, lors de tel événement, l'organisation fait face à une crise ? L'organisation en question, ou d'autres parties prenantes ?

Parmi tout l'éventail des définitions existantes de la crise, **j'ai sélectionné celles qui me paraissaient les plus pertinentes et adaptées au thème de la recherche.**

> Il y a plus de cinquante ans, Charles F. Hermann proposait une des premières définitions de la crise organisationnelle (Hermann, 1963). Il mettait en évidence trois caractéristiques de la crise (Frandsen et Johansen, 2017, p. 35) :
>
> - La menace
> - Le temps de réponse court
> - L'effet de surprise
>
> Plus tard, Thierry Pauchant et Ian I. Mitroff (chercheurs en gestion de crise) ont proposé une approche plus systémique de la crise organisationnelle : comment un système peut-il être bouleversé sous l'influence de plusieurs variables ? (Frandsen et Johansen, 2017, p. 36)
>
> La définition la plus répandue est sans doute celle établie par Pearson et Chair (1998) (Frandsen et Johansen, 2017, p. 36). Elle se distingue des autres définitions par les aspects importants d'une crise :
>
> - Un événement peu probable (avec beaucoup d'impact)
> - Une menace à la viabilité de l'organisation
> - Prise de décision rapide
>
> Les définitions précédentes sont assez générales, celles proposées par l'américain Timothy W. Coombs se rapprochent davantage du domaine de la communication de crise. La plus récente implique deux caractéristiques n'ayant pas été évoquées par les autres chercheurs : l'environnement lié à l'organisation et les parties prenantes

concernées par la crise. Sa définition met l'accent sur le concept de « perception », selon lequel un même et unique événement peut être interprété de différentes manières.

En 2011, Alpaslan et Mitroff prennent également en compte la perception des parties prenantes. Ils ajoutent à cela le caractère imprévisible d'une crise et la réaction en chaine qu'elle entraine.

Parmi toutes ces définitions, **mon choix s'est plutôt porté sur des concepts que sur une définition en tant que telle.** J'ai donc rassemblé les éléments les plus pertinents dans une nouvelle définition de la crise :

La crise pour une organisation est « *un processus rendu visible par un événement déclencheur (la plupart du temps non prévisible, mais pouvant être anticipé) occasionnant des menaces ou opportunités pour les performances de l'organisation, et créant un environnement d'incertitudes au sein duquel la maîtrise du temps et de l'information, tout comme la prise en compte des perceptions des parties prenantes, sont des enjeux déterminants pour une bonne gestion de crise* ».

2. De la criminalité à la cybercriminalité

Après m'être intéressée à la définition de la crise, un autre terme phare de ma recherche nécessitait d'être questionné : la cybercriminalité. **En quoi la cybercriminalité se différencie-t-elle de la criminalité traditionnelle ?**

Le centre européen de lutte contre le cybercriminalité d'Europol identifie quatre caractéristiques qui distinguent la cybercriminalité de la criminalité (European Cybercrime Center [EC3], 2014) :

1) ***The borderless nature*** : l'aspect « sans-frontière » d'internet permet à n'importe quel individu de commettre des crimes contre des gouvernements, entreprises, citoyens depuis l'autre côté de la planète.
2) ***The scalability*** : la facilité de perpétrer des crimes à grande échelle grâce à la standardisation des logiciels et la possibilité de toucher des millions d'ordinateurs sans contrainte logistique.
3) ***The ease to hide*** : la possibilité de réorienter le trafic en masquant l'origine de la fraude. Aussi, certains pays ont des compétences ou ambitions plus limitées pour lutter contre la cybercriminalité.
4) ***The nature of criminal cooperation*** : la complémentarité des compétences des criminels en réseau permet le développement d'une véritable économie parallèle.

La convention sur la cybercriminalité du Conseil de l'Europe définit la cybercriminalité comme **« l'ensemble des infractions commises contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques »** (Conseil de l'Europe, 2001). Cette convention donne une bonne indication de la variété d'infractions reprises sous la notion cybercriminalité.

Je refuse d'opposer la cybercriminalité à la criminalité traditionnelle**, elle se distingue plutôt par le vecteur utilisé que sont les systèmes informatiques, et par l'environnement virtuel** dans lequel le délit est commis.

Dans cette optique, le cyberhacking est considéré comme une forme de cybercriminalité car il vise à **forcer l'accès à un ordinateur, à modifier les données, à introduire des logiciels malveillants en exploitant des bugs et faiblesses des réseaux informatiques et humains pour y accéder de manière non-autorisée.**

3. Le cyberhacking, un type de crise

La notion de crise est définie et le concept de cybercriminalité est cerné. **Pouvons-nous désormais parler de crise de cyberhacking ? Oui, voici pourquoi** :

- Evénement déclencheur : cyberhacking visant les réseaux informatiques, divulgation d'informations, mise hors service de serveurs, etc.

> **Exemple** : dans mon échantillon, cet événement se traduit par différents types de cyberhacking. J'en ai identifié six :
>
> - Vol de données (Tumblr, MySpace, etc.) ;
> - Mise hors service d'un réseau (Deezer, Libération, etc.) ;
> - Défaçage (Malaysia Airlines, Canal +, etc.) ;
> - Extorsion de fonds (Tesco Bank, The DAO etc.) ;
> - Prise en otage de données (Netflix, Muni[2] etc.) ;
> - Usurpation d'identité (Colruyt, TV5 Monde, etc.).

- Non prévisible, mais pouvant être anticipé : grâce à la protection des réseaux, une veille sur les cyberhacking subis par les concurrents, etc.

> **Exemple** : Le réseau social russe VKontakte a été piraté entre 2011 et 2012. Les 100 millions de comptes ont été compris, car le site n'utilisait pas les normes de sécurité pour le stockage des mots de passe.

- Menaces ou opportunités sur les performances de l'organisation : Divulgation publique ou modifications de données confidentielles de clients. La réputation de l'organisation ainsi que la sécurité des clients

[2] Muni : San Fransisco Municipal Railway

sont en danger. En termes d'opportunités : amélioration des systèmes de sécurité des réseaux, bonne gestion de crise qui minimise l'impact réputationnel, visibilité, etc.

Exemple : en 2012, le réseau social Linkedin s'est fait dérober plus de 160 millions de données d'utilisateurs qui ont été mises en vente sur le darkweb par le groupe de hackers Peace of Mind. Dans sa communication, le réseau social dit avoir pris « des mesures importantes depuis 2012 pour renforcer la sécurité des comptes […] Nous avons ajouté des couches de protection supplémentaires au stockage des mots de passe et offrons la possibilité à nos membres d'activer la vérification en deux étapes pour plus de sécurité. » (Linkedin, 2012).

- Environnement d'incertitudes : quelle sera la réaction des victimes ? À quel point les données divulguées seront-elles médiatisées ? Combien de temps les serveurs seront-ils hors ligne ? Est-ce que les données pourront être décryptées ?

Exemple : Après 10 jours de statu quo, le centre médical presbytérien d'Hollywood a payé une rançon de 15.000 euros en 2016 pour récupérer les données de 900 patients rendues inaccessibles par les hackers. Une fois la rançon payée, l'hôpital a reçu une clé de décryptage lui rendant l'accès aux informations.

- Maîtrise du temps et de l'information : Cela concerne essentiellement les réponses à la crise. Quelles informations fournir aux parties prenantes ? Quand ? Comment communiquer sur les conséquences ?

Exemple : en 2016, Yahoo Mail a annoncé avoir « subi » plusieurs vagues de piratages concernant plus d'un milliard et demi de données. La mauvaise nouvelle, c'est que ces deux piratages datent en réalité de 2012 et 2016.

4. Le cycle de vie d'une crise

Précédemment, je me suis arrêtée sur les définitions qui cadrent les termes principaux utilisés dans mon mémoire. Désormais, j'ai besoin de situer mon analyse de la communication à un moment donné du processus de crise.

Les chercheurs et praticiens dans le domaine de la gestion de crise appliquent une approche par étapes en considérant une crise comme un cycle de vie. Ils divisent donc le processus de gestion de crise en plusieurs stades, aussi appelées « phases ».

Suivant les auteurs, le nombre de phases et leurs appellations varient. Fink (1986) et Lagadec (1991) en distinguaient quatre et Mitroff (1994) a élargi le modèle a cinq étapes. L'approche que je choisis est celle en trois phases de Timothy Coombs :

1) Pré-crise (détection du signal, prévention et préparation)
2) Crise (reconnaissance, confinement et restitution)
3) Après-crise (évaluation, mémoire institutionnelle et actions post-crise)

1.1. Avant la crise

Cette étape englobe toutes les actions préliminaires, les actions de prévention, de préparation et de détection de signaux ayant pour but de réduire les risques qui pourraient conduire à une crise.

Par exemple, Barton (2001) et Coombs (2006) suggèrent aux organisations d'adapter leur plan de gestion de crise annuellement, de désigner une équipe dédiée à la gestion de la crise, de tester les plans avec les équipes sur base d'exercices, etc. Ce plan est un outil de référence et non pas un guide étape par étape, car chaque crise est unique et suppose de prendre des décisions adaptées (Coombs, 2014).

1.2. Pendant la crise

Le deuxième stade représente la crise en tant que telle. Elle débute lorsque l'événement déclencheur survient et lorsque l'organisation prend conscience de la crise. **Concrètement, il s'agit de ce que les organisations font et disent lorsque la crise éclate**. Les relations publiques jouent un rôle important dans le développement des messages envoyés aux différents publics.[3] C'est à ce stade-ci que ma recherche se situe.

1.3. Après la crise

Dans la dernière phase de la crise, l'organisation donne généralement toutes les informations promises aux parties prenantes et analyse, tire des leçons de sa gestion de crise. **La crise n'est plus le centre d'attention de l'organisation, mais demande encore beaucoup de préoccupations**.

[3] http://www.instituteforpr.org/crisis-management-and-communications/

Le résumé du chapitre

Chapitre 1

les points clefs

« Toute étude sur les crises en vient à buter sur un problème de définition et de compréhension fondamentale : qu'entend-on par « crise » ? »
Lagadec, 1991

Ma définition de la crise

Evénement déclencheur — Menaces ou opportunités
Parties prenantes et incertitudes — Temps et information
Non prévisible, mais pouvant être anticipé — Processus

La cybercriminalité est une forme de **criminalité**

Le cyberhacking, **une crise ?**

OUI

Le cycle de vie d'une crise en 3 phases :

Avant

Pendant la crise

Après

II. La communication de crise

La première partie de ma recherche consistait en l'élaboration du contexte de la crise, et plus particulièrement d'une crise de cyberhacking. **Ce deuxième chapitre parcourt les théories principales en communication de crise**. C'est notamment ici que je vais présenter la théorie principale qui va nourrir ma recherche. **Je vais également mettre au point une deuxième typologie, celle des stratégies de réponse**.

1. Historique et définitions

La communication de crise est une discipline qui s'est développée très rapidement et cela se reflète dans les multiples théories de la communication de crise qui ont été développées ces dernières années.

- Années 80 : les premières publications traitent de la communication de crise et ont été écrites par des praticiens sur base de leur propre expérience ;
- Années 90 : les recherches en communication émergent avec, entre autres, trois théories importantes : Image Restoration Theory (Benoit, 1995), Corporation apology (Hearit, 1994) et Situation Crisis Communication Theory (Coombs, 1995) ;
- Années 2000 : Le champ de la communication de crise prend de l'ampleur avec notamment la Rhetorical Arena Theory (Frandsen & Johansen, 2007) ;
- Années 2010 : la communication digitale s'installe avec la globalisation.

Sturges (1994) est l'un des rares et premiers chercheurs à se concentrer sur le contenu d'une stratégie de communication lors d'une crise en distinguant trois types d'information :

- « Instructing information » : l'information qui informe les individus sur la façon de réagir physiquement à la crise.

- « Adjusting information » : l'information qui aide les individus à se protéger psychologiquement des conséquences de la crise.
- « Internalizing Information » : l'information que les individus utiliseront pour se représenter l'image de l'organisation.

Ces trois types de communication sont présentés séparément, mais en réalité, se combinent de différentes manières selon le stade du cycle de vie de la crise. **Les deux premiers types de communication jouent un rôle important pour ma recherche car ils définissent la stratégie initiale** que chaque organisation peut mettre en place dès que la crise survient. J'y reviendrai plus en profondeur dans la partie dédiée à la Situational Crisis Communication Theory de Timothy Coombs.

Selon Frandsen & Johansen, la communication de crise peut être définie à partir des phases de son cycle de vie ou du contenu, des fonctions qu'elle peut avoir. **Ils définissent la communication de crise comme *« a complex and dynamic configuration of communication processes - before, during, and after a crisis - where various actors, contexts and discourses (manifested in texts) are related to each other (instructing, adjusting and internalizing) ».***

2. Les théories en communication de crise

Les théories de la communication de crise décrivent, expliquent et recommandent comment et pourquoi communiquer lorsque les organisations font face à différents types de situations de crise. J'ai sélectionné trois théories intéressantes :

a) Image Restoration Theory (IRT) de William Benoit
b) Situational Crisis Communication Theory (SCCT) de Timothy Coombs
c) Rhetorical Arena Theory (RAT) de Finn Frandsen et Winni Johansen

2.1. Image Restoration Theory (W. Benoit)

Le Nord-Américain William L. Benoit a développé une **théorie sur la manière dont les individus et les organisations communiquent et se défendent lorsque leur réputation est menacée.** Il a identifié des stratégies de défenses verbales utilisées pour réparer une réputation qui aurait été endommagée lors d'une crise :

- Déni
- Fuite des responsabilités
- Réduction de l'offense
- Mesures correctives
- Affront

Les organisations sélectionnent et combinent plusieurs stratégies, mais certaines conviennent mieux que d'autres en fonction de la situation. Par contre, le silence ne fait pas partie de ses stratégies, car il le considère comme une stratégie non-verbale.

Deux critiques ont été faites au sujet de cette approche :

1) Elle néglige l'aspect dynamique d'une image qui se construit dans l'esprit du récepteur ;
2) Il serait impossible, peu importe les stratégies, de retrouver exactement la même image. Par contre, construire une nouvelle image positive de l'organisation est envisageable.

2.2. Situational Crisis Communication Theory (T. Coombs)

Comme la théorie précédente, la SCCT s'interroge sur **le rôle de la communication dans la protection de la réputation d'une organisation en crise.** Là où l'approche de Coombs diffère de la précédente, c'est dans ses efforts de contextualisation.

La théorie de l'attribution, issue de la psychologie sociale, est au cœur de l'approche de Coombs. Elle part du principe que chaque individu cherchera d'autant plus d'explications et de responsables si l'événement sur lequel il s'interroge engendre des conséquences négatives. La théorie de l'attribution c'est :

- L'attribution de la responsabilité à quelqu'un (l'organisation),
- Par des individus (les parties prenantes),
- Pour un événement donné (une situation de crise).

Dès lors, à quel point l'organisation est-elle responsable de la crise ? C'est à partir de ce questionnement que Coombs construit son approche. Selon lui, **plus l'organisation sera responsable, plus l'atteinte à sa réputation sera grande. Il s'interroge donc sur les facteurs qui influencent l'attribution de cette responsabilité pour ensuite proposer les stratégies de réponses les plus adéquates afin de minimiser l'atteinte à la réputation.**

Dans le cadre de ma recherche, je me suis appropriée certains éléments de sa théorie. À savoir, l'influence de cette attribution sur les stratégies de réponse. J'ai volontairement écarté le volet consacré à la protection de la réputation qui se situe davantage dans la phase d'« après-crise ».

Le processus est donc le suivant :

A. **Quel type de crise ?** Victime, accidentelle ou prévisible
B. **Quels facteurs d'amplification ?** Antécédents de crise, relation avec les parties prenantes, gravité de la crise
C. **Quel degré de menace pour la réputation ?** Attribution faible, modérée ou élevée
D. **Quelle stratégie de réponse ?** Déni, minimisation, reconstruction, renforcement

En vert, les éléments que je m'approprierai. En rouge, ceux que je laisse de côté. Désormais, je vais donc développer les points qui concernent ma recherche.

A. L'identification du type de crise

Pour Coombs, le type de crise influence la façon dont les individus vont attribuer la responsabilité de la crise à l'organisation. Chaque type représente donc un niveau spécifique de responsabilités, et identifier le type de crise me permettra de comprendre les responsabilités de l'organisation. Comment ? En y associant la méthode de cyberhacking.

- **La victime** : l'organisation obtient le statut de victime de la crise, peu de responsabilités lui sont attribuées par les parties prenantes et donc la menace à la réputation est faible.

> **Exemple** : J'associe ce type de crise au cyberhacking de type DDoS (Distributed Denial of Services) et dans certains cas d'usurpations d'identité, mais cela ne concerne que 10% de l'échantillon. C'est le cas du cyberhacking qu'a connu l'hébergeur Dyn en 2016 lorsque des sites tels que Netflix, Twitter, Spotify, Amazon ont été rendus inaccessibles pendant plusieurs heures.

- **La crise accidentelle** : des actions involontaires de l'organisation ont mené à la crise, mais d'autres facteurs en sont également responsables. Peu de responsabilités sont donc attribuées à l'organisation et la menace à la réputation est modérée.

> **Exemple** : ce type de crise est rencontré par 30% des organisations de l'échantillon. Des méthodes telles que l'ingénierie sociale[4] caractérise ce type de crise. Par exemple, les données de 133.000 clients de l'opérateur britannique Three Mobile ont été volées en 2016 suite à une campagne de phishing qui a permis aux hackers d'entrer dans les systèmes de la société.

[4] La particularité de l'ingénierie sociale consiste en l'exploitation d'une faille, non pas au sein de systèmes informatiques, mais une faille humaine. La cible c'est l'internaute qui, naïvement, donne accès à ses informations personnelles. Il s'agit donc d'abuser de la confiance d'un individu en profitant d'une erreur humaine.

- **La crise prévisible** : les parties prenantes croient fermement que l'organisation est responsable de la crise et que cette crise aurait pu être évitée, voire que l'organisation s'est volontairement engagée dans des situations à risques pour les individus. Dans ce cas, l'attribution est forte et la menace à la réputation est élevée.

> **Exemple** : dans les cas de cyberhacking, on parlera de crise prévisible lorsqu'il s'agit d'une faille de sécurité dans un système informatique ou lorsque les informations sont trop faiblement protégées. Une crise de cyberhacking sur trois est prévisible et concerne essentiellement les vols. Linkedin, qui s'est fait dérober en 2012 plus de 160 millions de données par le groupe de hackers Peace of Mind, chiffrait ses données de manière très faible en utilisant un algorithme réputé peu fiable par les spécialistes en informatique.

B. Les facteurs d'amplification

Coombs identifie trois facteurs qui amplifient les responsabilités de l'organisation en crise :

a) Les antécédents : l'organisation a-t-elle déjà connu une crise similaire ?
b) La réputation négative : dans quelle mesure la relation avec les parties prenantes était-elle dé(favorable) ?
c) La gravité de la crise : à quel point la crise est-elle grave ?

> **Exemple** : je n'aborde pas le point qui concerne la réputation. Par contre, celui de la récidive (antécédents) est intéressant. Au minimum quatre organisations sur dix avaient déjà vécu une crise de cyberhacking auparavant. De plus, la gravité de la crise a été mesurée en fonction du type de cyberhacking et influence certaines stratégies communicationnelles.

En résumé, des antécédents de crise, une relation défavorable et une crise d'une grande ampleur intensifient l'attribution des responsabilités et a un effet direct sur la réputation de l'organisation (Coombs, 2004a ; Coombs & Holladay, 2001).

Ces attributions causales sont importantes lors du choix de la stratégie de réponse, car Coombs et Holladay (2006) ont identifié trois conséquences de l'attribution de la responsabilité : (1) un impact négatif sur la réputation de l'organisation (2) une modification du comportement d'achat, et (3) un bouche-à-oreille négatif.

C. Les stratégies de réponse

Dès lors, comment réagir de manière efficace en tenant compte de cette attribution des responsabilités ?

Coombs propose une réponse initiale qui peut être communiquée dans les plus brefs délais, peu importe le type de crise. Comme mentionné précédemment, cette réponse de base est composée de deux volets :

1) Les instructions : informer les parties prenantes sur les actes à poser pour se protéger physiquement de la crise.
2) L'information d'adaptation : aider psychologiquement les victimes.

Exemple : Dans le cas de crises de cyberhacking, les deux volets de la réponse initiale se manifestent sous différentes formes et sont mis en place dans 99% des cas :

- Les instructions : conseils pour mieux protéger ses identifiants personnels, mises en garde par rapport aux méthodes d'ingénierie sociale, énumération chronologique que des faits.
- L'adaptation de l'information : rassurer les victimes en insistant sur l'importance que la marque accorde à la confiance de sa clientèle, mettre en avant la collaboration avec des équipes d'experts, les forces de l'ordre, etc.

Cette réponse initiale permet donc d'instaurer un climat de contrôle de la crise par l'organisation vis-à-vis des parties prenantes.

Selon Lagadec, trois types de messages peuvent structurer la communication initiale :

- « Nous sommes avertis du problème et nous l'avons pris en charge, dans toutes ses dimensions, tant techniques qu'organisationnelles, humaines et sociales. »
- « De nombreuses inconnues subsistent, mais tout est mis en œuvre pour réunir des informations complémentaires, et traiter la situation : les plans d'urgences ont été activés, et voici précisément comment ils fonctionnent. »
- « Des informations seront données dès que l'on en apprendra davantage. »

Figure1. Le tweet de la BBC lors du piratage de son site web en 2015.

Pour illustrer cette communication initiale selon Lagadec, le tweet ci-contre nous montre ce qu'a répondu la BBC lors du piratage de son site web en 2015.

Au-delà de la réponse initiale, les organisations peuvent choisir d'autres stratégies de réponses plus élaborées. Dans ses stratégies de réponse aux crises, Coombs fait une distinction entre quatre postures : le déni, la minimisation, la reconstruction et le renforcement. Une organisation n'émettra pas qu'un seul et unique message, d'un seul et même type. Plusieurs stratégies peuvent être combinées. Cependant, la cohérence est importante.

La procédure de correspondance décrite dans le tableau ci-dessous est la synthèse de la théorie de Coombs. **En fonction du type de crise et des facteurs d'amplification, les parties prenantes vont attribuer un niveau de responsabilité à l'organisation qui réagira ensuite par le biais de stratégies de réponses.**

<table>
<tr><th colspan="4">Procédure de correspondance</th></tr>
<tr><th>Type de crise</th><th>Facteurs d'amplification</th><th>Attribution</th><th>Stratégie de réponse</th></tr>
<tr><td colspan="4">Réponse initiale
Pour toutes les crises, première étape de la stratégie de réponse</td></tr>
<tr><td>Rumeurs, challenges</td><td>Non</td><td>Faible à modérée</td><td>Stratégie de déni
Uniquement si bonnes justifications, preuves. La stratégie du déni est généralement déconseillée.</td></tr>
<tr><td>Accidentelle</td><td>Non</td><td>Elevée</td><td rowspan="2">Stratégie de réduction</td></tr>
<tr><td>Victime</td><td>Oui et non</td><td>Faible</td></tr>
<tr><td>Accidentelle</td><td>Oui</td><td>Faible</td><td rowspan="2">Stratégie de reconstruction
Pour n'importe quelle crise prévisible</td></tr>
<tr><td>Prévisible</td><td>Oui et non</td><td>Elevée</td></tr>
<tr><td colspan="4">Stratégie de renforcement
Pour compléter d'autres stratégies (stratégie de victimisation uniquement utilisée s'il s'agit d'une crise où l'organisation est également une victime)</td></tr>
</table>

Les types de discours en temps de crise sont variés et beaucoup de typologies de réponses comme celle de Coombs (2014) ont été créées (Lagadec, 1986 ; Westpphalen, 1997 ; Benoit, 2004). La typologie de réponse utilisée pour ma recherche est un mélange de la typologie proposée par Coombs et par Libaert.

La typologie de Libaert repose sur trois axes :

a) Les stratégies de la reconnaissance : acceptation de la responsabilité par l'entreprise abordée sous l'angle de la théorie des jeux. Elles seraient les plus efficaces mais sont peu utilisées car les organisations rencontrent beaucoup de contraintes internes.
b) Les stratégies du projet latéral : l'organisation déplace le point du problème pour l'aborder sous un angle nouveau.
c) Les stratégies du refus : à l'opposé de la reconnaissance mais ne signifie pas nécessairement un rejet total de communication.

À partir de ces deux typologies, voici celle qui sera utilisée dans le cadre de ce mémoire :

Typologie des stratégies de réponse	
Stratégies	**Exemples**
Réponse initiale	○ Protéger physiquement les parties prenantes des conséquences de la crise ○ Protéger psychologiquement les parties prenantes du stress que provoque une crise
Déni	○ Pas de communication (silence) ○ Nier l'existence d'une crise ○ Nier ses responsabilités par rapport à la crise ○ Nier ses responsabilités et désigner d'autres responsables
Projet latéral	○ Déplacer la communication vers un autre sujet ○ Accepter certaines responsabilités, mais impliquer d'autres responsables ○ Accepter certaines responsabilités, mais avec circonstances atténuantes ○ Se positionner en tant que victime
Reconnaissance	○ Accepter toutes les responsabilités et présenter ses excuses
Reconstruction	○ Rappeler ses bonnes actions ○ Dédommagement des victimes ○ Prévention (éviter que cela ne se reproduise)

Exemple : dans l'échantillon, la stratégie de réponse la plus répandue est celle du projet latéral contrairement à la stratégie de reconnaissance qui est presque inexistante.

Finalement, toutes ces stratégies constituent l'argumentation de l'organisation et ne sont pas les seuls paramètres qui déterminent la réussite en gestion de crise. En effet, la communication de crise est un élément important de cette gestion, mais les capacités à la fois techniques,

économiques, relationnelles, etc. de gérer cette crise sont des facteurs clefs. En annexe se trouvent des exemples de ces stratégies de réponses mises en place par les organisations de l'échantillon.

2.3. Rhetorical Arena Theory (F. Frandsen & W. Johansen)

Frandsen et Johansen reprochent aux deux approches précédentes de négliger la complexité des crises, de ne pas prendre en compte toutes les « voix » qui communiquent en situation de crise et donc d'être exclusivement axées sur la communication de l'organisation.

- **Benoit** : approche de la communication de crise en tant que stratégies de restauration de l'image. Comment les organisations font face à une menace vis-à-vis de leur réputation (Frandsen et Johansen, 2007) ?

- **Coombs** : approche de la communication de crise en tant que « relationship management ». Comment la relation entre l'organisation et ses parties prenantes (attribution causale) ont un impact sur les activités de communication de l'organisation pendant la crise (Frandsen et Johansen, 2007) ?

Ces deux chercheurs proposent donc un nouveau modèle de communication de crise qui ne remplace pas les précédents, mais qui les complètent en prenant en compte toutes les voix de « l'arène ». La prise en compte de ces voix apporte un sens nouveau, de nouvelles interprétations. Comment les individus interagissent-ils entre eux et avec l'organisation ? Comment les employés réagissent-ils ? Comment les médias couvrent-ils la crise ?

3. Les enjeux en communication de crise

Les théories présentées ci-dessus traitent toutes des mêmes enjeux. Avant d'entamer l'analyse en tant que telle, **je trouvais intéressant d'avoir une vision globale de ces enjeux impliqués lors de la communication en temps de crise et qui guideront l'interprétation des résultats**.

3.1. La gestion du temps

Lorsque la crise éclate, beaucoup d'organisations hésitent à communiquer. Le risque dans ce genre de situation est que d'autres acteurs posent des mots sur la crise. Communiquer rapidement ne nécessite pas de posséder toutes les informations mais permet d'éviter la position défensive en donnant sa version des faits. Nous le verrons dans les résultats, les organisations ont des politiques très différentes en matière de gestion du temps et des délais de communication.

Exemple : Yahoo a nié l'existence d'un piratage datant de 2012, où plus de 200 millions de données d'utilisateurs ont été compromises. Le site spécialisé Motherboard[5] a révélé la fraude avant que Yahoo ne confirme les faits. La marque a déclaré être au courant d'une possible mise en vente des données, mais n'en n'a pas informé les utilisateurs.

3.2. La tonalité de la communication

Thierry Libaert distingue deux écoles en ce qui concerne la tonalité de la communication :

1) **L'école rationaliste** ou technicienne qui communique sur des faits réels (dates, quantités, volumes) ;
2) **L'école symboliste** ou communication qui utilise les valeurs, images et émotions.

[5] https://motherboard.vice.com/fr

Exemple : Je remarque que dans le cas de crises de cyberhacking, en particulier lorsqu'il s'agit d'un vol de données, les organisations communiquent presque exclusivement sur des faits, tel que décrit par l'école rationaliste. Il s'agit par exemple de la chronologie des événements, de son ampleur, des mesures mises en place pour se protéger. L'aspect humain est très peu mis en avant.

3.3. La cohérence des messages

Lorsqu'il parle de cohérence, Coombs insiste sur le caractère unifié de la réponse donnée aux parties prenantes. Cela ne signifie pas qu'une seule personne ne prenne la parole. Il s'agit plutôt de parler d'une même voix, à l'unisson.

Exemple : le choix de l'ambassadeur dans les crises de cyberhacking concerne généralement une personne exerçant un métier lié au domaine de la communication. Aussi, il fréquent de voir que l'organisation ne désigne pas un porte-parole particulier, mais elle communique en son propre nom. Le plus frappant c'est le choix de l'expert en sécurité informatique, mais uniquement dans le secteur internet. Il intervient régulièrement lors de crises de cyberhacking dans ce secteur, mais presque jamais lorsque ces crises touchent d'autres domaines d'activité.

Au final, **« toute la problématique de la communication de crise, c'est qu'elle n'obéit à aucun véritable paradigme : ainsi, la même méthode utilisée en un endroit avec succès s'avère catastrophique en un autre lieu »** (Heiderich, 2010, p. 75). Thierry Libaert (2015) ajoute qu'« il n'existe pas de modèle général de réussite, une méthode de communication ayant parfaitement réussi à surmonter une crise au sein d'une entreprise peut échouer rapidement dans une autre organisation pourtant confrontée au même enjeu. Il est d'ailleurs caractéristique de constater, au sein d'une même entité, des cycles de réussites et d'échecs ».

Le résumé du chapitre

III. Approfondissement du concept de cyberhacking

1. Typologie des crises de cyberhacking

Pour mon analyse, **j'ai désormais besoin de creuser ce concept de cyberhacking en parcourant les modes opératoires, le profil des hackers et en élaborant une typologie pertinente car ces éléments peuvent influencer la communication de l'organisation.**

Dans la littérature académique, **beaucoup de chercheurs ont mis au point des typologies en fonction des spécificités de la crise.** Par exemple, une typologie sur base du contenu de la crise (Coombs, 1999 ; Alpaslan & Mitroff, 2011), de ses causes (Rosenthal et al. 2011b) ou conséquences (Drennan & McConnell, 2007, cité par Frandsen et Johansen, 2016). Dans son ouvrage « La communication de crise », Thierry Libaert propose également sa propre typologie des crises qu'il classe en quatre sphères. Thimothy Coombs a énormément contribué à la recherche des typologies de crises dans sa Situational Crisis Communication Theory (SCCT) (Coombs, 2015).

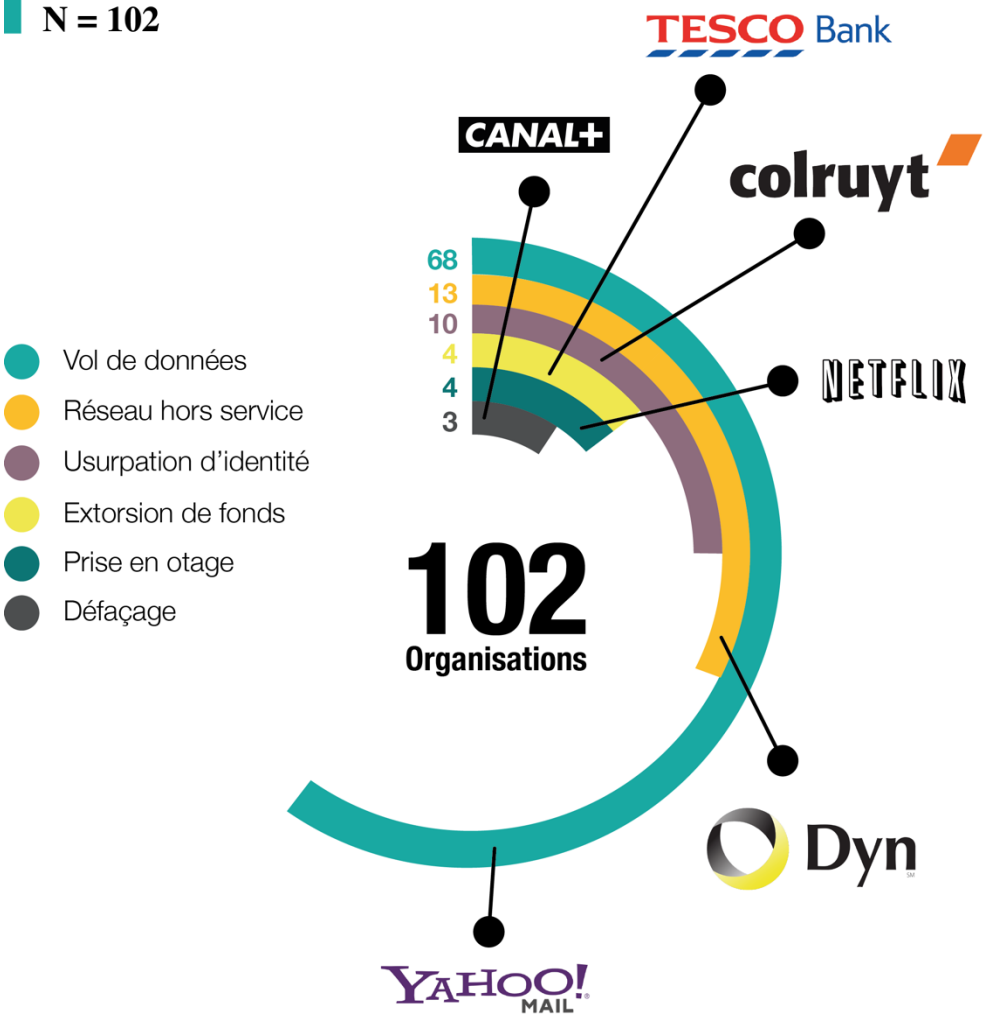
Les typologies énumérées précédemment sont très générales, car les crises de cyberhacking sont déjà un sous-ensemble de crises. Des tentatives en matière de mise au point d'une typologie propre aux crises de cyberhacking existent, mais je construirai mon analyse à partir de ma propre typologie. Comme le souligne Thierry Libaert (2015), « il n'existe pas de mauvaises typologies, il n'y a que des mauvaises utilisations ».

Typologie des crises de cyberhacking	
Typologie	**Exemples**
Vol de données	**Yahoo!** : plus de 110 millions d'identifiants ont été dérobés et revendus sur le dark web en mai 2012 (données non bancaires).
Réseau hors service	**Dyn** : attaque par déni de service à partir d'objets connectés qui a bloqué l'accès à de nombreux sites (Netflix, Spotify, Twitter, PayPal, Playstation network, Airbnb…) en octobre 2016.
Extorsion de fonds	**Tesco Bank** : 2,8 millions d'euros dérobés en novembre 2016 suite à des transactions frauduleuses provenant de 9000 comptes en ligne.
Usurpation d'identité	**Colruyt :** En 2017, des emails promotionnels ont été envoyés aux clients du groupe Colruyt à partir de fausses adresses électroniques, ressemblant à celles utilisées par le groupe, afin de récupérer des données privées voire bancaires.
Prise en otage de données	**Hollywood Presbyterian Medical Center** : cet hôpital de Los Angeles a dû payer 17.000 dollars aux pirates pour récupérer les données des patients rendues inaccessibles par un virus informatique.
Défaçage	**Malaysia Airlines :** le site de la compagnie aérienne a été piraté en 2015 par Lizard Squad. Un message en référence à la disparition du vol MH370 s'affichait sur le site : « 404 - avion non trouvé ».

Le cœur de l'analyse arrivera plus tard, mais je souhaite faire une parenthèse en présentant quelques résultats pertinents pour ce chapitre. Cette typologie m'a en effet permis de trier les 102 crises de mon échantillon. **Le vol de**

données est le type de crise le plus représenté. Un peu moins de la moitié de ces vols concernent des données bancaires. L'ampleur des vols oscille, mais le record est actuellement détenu par Yahoo et son milliard de données volées en 2013.

Figure 2. Les organisations réparties en fonction du type de cyberhacking.
N = 102



2. Les modes opératoires d'un cyberhacking

Lors de chaque crise de cyberhacking, la méthode utilisée par le hacker pour arriver à ses fins varie. Une même méthode peut être utilisée lors de deux types de crises différents. Tout comme un même type de crise peut résulter de méthodes différentes.

Je m'intéresse à ces modes opératoires car **ils vont me permettre de situer la responsabilité de l'organisation vis-à-vis de la crise**. **Cette responsabilité peut ensuite influencer la communication de l'organisation.**

- « Phishing » (hameçonnage) ou « social engineering » : infraction en ligne cherchant à induire l'utilisateur en erreur pour lui soutirer des informations identitaires ou bancaires à différentes fins.

  Exemple : de nombreux clients de Colruyt ont récemment reçu des e-mails promotionnels depuis une adresse semblable à celle du groupe, mais ayant pour but de tromper les destinataires et de récolter leurs informations.

  Les données récupérées peuvent également être utilisées comme porte d'entrée au sein d'une infrastructure plus vaste, par exemple en utilisant les identifiants d'un individu pour pénétrer dans les systèmes informatiques d'une tierce partie.

  Exemple : Un employé de l'organisation de télécommunications britannique Three Mobile s'est fait dérober ses identifiants au travers d'une opération d'hameçonnage. Avec ces identifiants, les pirates se sont introduits dans les systèmes informatiques de l'organisation et ont subtilisé une centaine de milliers de données clients.

- « Denial of Service » (attaque par déni de service) : opération qui « vise à rendre un serveur, un service ou une infrastructure indisponible en surchargeant la bande passante du serveur, ou en accaparant ses ressources jusqu'à épuisement »[6]. Ces dénis sont dits distribués, car la source de ces attaques est constituée de réseaux d'ordinateurs infectés par un virus et présents partout dans le monde, un « botnet ».

[6] https://www.ovh.com/fr/anti-ddos/principe-anti-ddos.xml

Exemple : Le site d'hébergement internet OVH a été ciblé par ce type de méthode en septembre 2016. Les serveurs n'ont pas résisté aux vingt-six offensives lancées simultanément, certaines atteignant plus de cent gigabits par seconde (volume de trafic envoyé vers le serveur), un record pour l'époque. Cette méthode est utilisée dans 13% de l'échantillon.

- **«** Cracking **»** : contourner la protection d'un logiciel, de systèmes pour l'utiliser sans payer la licence qui s'y rapporte. Ici, il sera surtout défini comme un moyen de deviner les identifiants (login et mots de passe) d'un utilisateur, pénétrer dans un système informatique en utilisant ses failles physiques.

Exemple : The DAO, organisation spécialisée dans la crypto-monnaie a été délestée de plus de cinquante millions de dollars suite à une intrusion dans son système. Le pirate a exploité une faille du code de The DAO.

- « Malware » : programme malveillant (vers, virus, chevaux de Troie, spyware…) qui s'introduit dans un ordinateur à l'insu de l'utilisateur pour perturber le système informatique. Il est souvent installé lors du téléchargement d'une pièce jointe provenant d'un destinateur peu fiable, lors de visites sur des sites illégaux, etc.

Exemple : Le malware Mirai a provoqué d'importantes pannes de réseau chez l'opérateur Deutsche Telekom l'année dernière. En infectant des objets connectés, il a exploité une vulnérabilité présente dans les routeurs internet et a propagé le virus à d'autres routeurs très rapidement.

Les ransomware (rançons logiciels) font partie de cette famille, car il s'agit de chevaux de Troie destinés à extorquer les individus. Ce logiciel malveillant infecte l'ordinateur et crypte les données. Pour débloquer l'accès aux données, le hacker à l'origine du délit demande une rançon à l'utilisateur. Parmi ces ransomware, les plus connus sont

WannaCrypt, CryptoLocker, CryptoWall et Locky, mais il en existe beaucoup d'autres.

Exemple : Le centre médical presbytérien d'Hollywood a payé une rançon de 15.000€ pour récupérer les données de ses patients après dix jours de statu quo.

Il ne s'agit pas d'une liste exhaustive des différentes méthodes utilisées par les pirates informatiques. En effet, d'autres moyens tels que le « spoofing », « pharming », « man in the middle » existent et sont mis en pratique.

Ces modes opératoires évoluent quotidiennement et ne cessent de défier l'adaptation des organisations en matière de sécurité informatique. Lorsqu'un virus du domaine médical mute, il remet en question les traitements existants. C'est le même procédé en ce qui concerne les virus informatiques qui se multiplient et se diversifient à très grande vitesse.

Tout comme il existe différents types de cyberhacking, **il existe différents profils de hackers** en fonction de leurs motivations, ressources et compétences :

- « White Hat » : ils aident les organisations à repérer et réparer les failles dans des systèmes informatiques. Ils sont généralement employés par cette organisation et agissent en toute légalité.
- « Black Hat » : ils accèdent illégalement aux systèmes informatiques et en compromettent la sécurité. Ils représentent la quasi-totalité de mon échantillon.
- « Grey Hat » : à mi-chemin entre les chapeaux blancs et noirs, ils agissent illégalement mais n'ont pas pour objectif d'endommager un système. Ils avertissent généralement les organisations lorsqu'ils trouvent une faille.

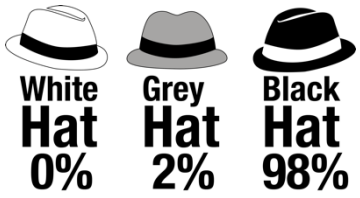
Exemple : Lors des piratages de Plenty of Fish (2011) et Pirate Bay (2010), le hacker argentin Chris Russo a récupéré les

informations de millions d'utilisateurs sans les mettre en ligne. Il a ensuite prévenu les administrateurs de la faible protection de ces données et a proposé de travailler avec eux.

S'ajoutent à ces trois grandes catégories de hackers, de multiples sous-catégories. Par exemple :

- « Script Kiddies » : sont rassemblés dans cet ensemble les utilisateurs débutants qui profitent et s'attribuent les programmes prêts à l'emploi de hackers plus expérimentés.
- « Hacktivistes » : ces personnes commettent des délits informatiques et sont motivées par une idéologie (politique, sociale, religieuse…) (ex : Anonymous).

Figure 3. Les profils de hackers présents dans l'échantillon d'analyse.
N = 39



À l'exception de Chriss Russo, tous les pirates informatiques à l'origine des piratages de mon échantillon appartiennent à la catégorie des « Black Hat ».

Leurs motivations sont diverses et peuvent permettre aux organisations d'orienter leur communication différemment. Les objectifs les plus fréquents sont :

1) L'argent (MySpace, 2013)
2) Les revendications politiques, religieuses, etc. (Sony, 2012)
3) Dévoiler l'incompétence, les failles d'une organisation (VTech, 2015)
4) La dénonciation de pratiques (Ashley Madison, 2015)
5) La vengeance personnelle (Libération, 2013)
6) Le plaisir (Dyn, 2016)

Le résumé du chapitre

Chapitre 3

les points clefs

« Il n'existe pas de mauvaises typologies, il n'y a que des mauvaises utilisations »

Libaert, 2010

Une **typologie** des crises de **cyberhacking**

- Vol de données
- Extorsion de fonds
- Réseau hors service
- Prise en otage de données
- Défaçage
- Usurpation d'identité

Le **PROFIL** des hackers

White Hat Grey Hat Black Hat

Eléments qui orientent la **communication**

La **MOTIVATION** des hackers

Argent	Dénoncer des pratiques
Vengeance	Dévoiler la faille
Plaisir	Revendications

IV. Méthodologie et limites

J'ai choisi d'utiliser la méthode d'analyse de cas qui consiste à collecter « un ensemble de données empiriques » (Bichindaritz cité par Leplat, 2002, para. 4). Chaque cas constitue une unité d'analyse qui s'inscrit dans un contexte qui lui est propre pour mettre au jour ses particularités. Cela permet d'apporter différentes solutions à une même situation en articulant différentes méthodes. « C'est le mode de conjonction de ces méthodes qui est l'objectif visé » (Leplat, 2002, para. 13), comme le souligne Hamel: « la variété des méthodes s'inscrit dans ce but de croiser les angles d'étude ou d'analyse » (Hamel cité par Leplat, 2002, para. 13). Dans cette optique, la « triangulation des données » vise à déterminer un « canevas à partir duquel pourront être situés les différents éléments d'un terrain et de ce fait, croiser les points de vue et tisser un réseau qui fera apparaître l'organisation du cas » (Leplat, 2002, para. 14). La difficulté de l'étude de cas est de démontrer le caractère scientifique et rigoureux de cette démarche, mais elle d'autant plus intéressante, car elle évite le versant subjectif de certains discours. Le but étant de **repérer, dans les discours des organisations, les stratégies de communication que ces dernières ont mises en place en fonction de différentes variables** (type de cyberhacking, profil du hacker, secteur de l'organisation, etc.).

L'échantillon comporte **102 cas de cyberhacking**, produits entre 2010 et 2017 et concernant **80 organisations différentes**. Mon corpus est composé des informations trouvées dans la presse francophone en ligne. Ma grille d'analyse est divisée en trois thèmes, comportant chacune plusieurs variables.

Figure 4. Un extrait de la grille d'analyse du corpus.

Données propres à l'organisation					
Nom de l'organisation cible	Secteur d'activité	Siège social			
Données propres au cyberhacking					
Type de cyberhacking	Gravité de la crise	Mode opératoire	Type de crise (Coombs)	Profil et motivations du hacker	
Données propres à la communication					
Année où le hacking a eu lieu	Année où le hacking a été dévoilé	Délai de communication	Ambassadeur	Canal de communication	Stratégies de réponse

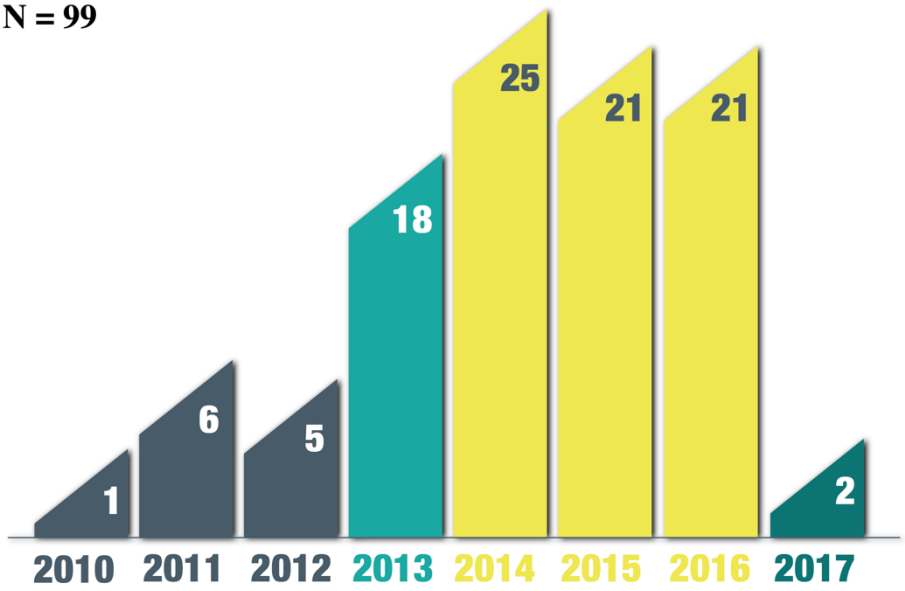
La grille ci-dessus est un extrait des variables qui ont été prises en compte pour chacun des cas de mon échantillon. Ce tableau a donc été reproduit 102 fois et pour chacune des crises, **quatorze variables ont été observées**. Lorsque qu'une des caractéristiques ne trouvait pas de réponse, j'ai indiqué la mention « N/A » (*no answer* ou *not available*). C'est pour cela que chaque graphique est accompagné du taux de réponse (N = …).

Deux variables supplémentaires avaient été intégrées à cette grille, mais n'ont finalement pas abouti **:** la visibilité de la crise et son coût. Dans un premier temps, la visibilité a été mesurée sur une échelle de 0 à 20. Le nom de l'organisation suivie du terme « piratage » était soumis à un moteur de recherche (Google). Chaque résultat de recherche abordant le sujet était comptabilisé, et ce comptage était effectué sur les vingt premiers résultats (deux premières pages de la recherche). N'étant pas convaincue de la méthode pour juger sur base du web, j'ai préféré utiliser ces indices de visibilité à titre indicatif, en les laissant en marge du corps de l'analyse. Il serait tout de même intéressant d'approfondir cette variable en se demandant ce qui rend une crise visible. Quels sont leurs caractéristiques et points communs ? Qu'est-ce qui rend une crise plus visible qu'une autre ? Les coûts d'une crise de cyberhacking sont difficiles à mesurer et requièrent une méthodologie précise. En effet, certaines organisations expliquent le manque de sécurité informatique par le coût que cela implique. Cette remarque est-elle légitime comparée aux coûts que représente la gestion d'une crise ?

Je m'intéresse donc à la Situational Crisis Communication Theory de Timothy Coombs en adaptant certains aspects de sa théorie à mon analyse comme le type de crise, sa gravité, les antécédents, et l'attribution de la responsabilité. L'état de la relation avec les parties prenantes et l'aspect lié à la réputation sont laissés en marge de l'analyse.

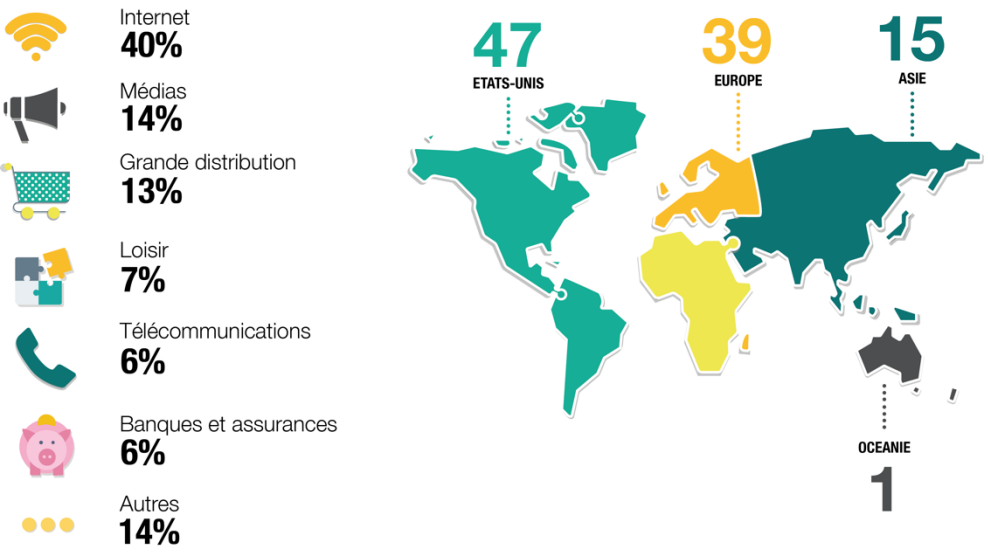
Pour cette recherche, les unités sélectionnées sont celles qui correspondent à cette **définition de l'organisation** : « ensemble structuré d'individus en interaction poursuivant un but collectif ». Suivant cette définition, 102 cas ont été récoltés sur la scène médiatique francophone en ligne. Les communications officielles des organisations (en français ou en anglais) ont également été prises en compte.

Figure 5. Le nombre de crises de cyberhacking par année.
N = 99



Avant d'éplucher les résultats d'analyse, il est intéressant d'avoir à l'esprit l'année où les crises se sont produites. Un quart des crises de mon échantillon se sont produites en 2014.

Figure 6. Les organisations en fonction de leur secteur et siège social.
N = 102



La plupart des organisations sont originaires du continent américain et européen. Les secteurs les plus représentés sont ceux de l'internet, de la grande distribution et des médias.

Mon corpus se compose d'informations médiatisées. Les plus petites structures sont donc moins présentes et certains cas de cyberhacking, comme la prise en otage de données, sont moins représentés. Des biais sont donc à prendre en compte lors de l'analyse car ce n'est pas parce que certaines segmentations sont peu représentées qu'elles sont peu fréquentes en réalité.

Le résumé du chapitre

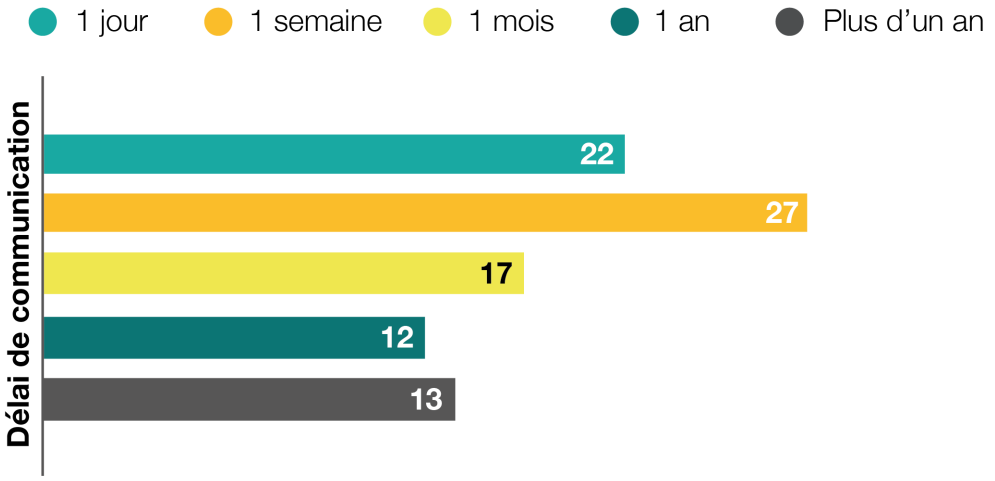
V. Les stratégies communicationnelles lors de crises de cyberhacking

Tous les éléments théoriques dont j'avais besoin pour nourrir l'analyse des résultats ont été présentés. Dans ce chapitre, **j'identifie les comportements communicationnels des organisations ayant vécu des crises de cyberhacking.**

1.1. Le délai de communication

Parmi les enjeux en communication de crise, j'avais pointé celui de la gestion du temps. Je me suis donc interrogée sur le délai entre le moment où la crise survient, et le moment où l'organisation réagit. **La plupart du temps, les organisations communiquent dans le mois ayant suivi la crise.**

Figure 7. Les organisations en fonction du délai de communication.
N = 91



Lors d'un vol de données, ce délai de communication varie avec la gravité de la crise car **plus la quantité de données volées augmente, plus l'organisation patiente avant de communiquer.**

Le secteur des médias est le plus rapide dans sa communication car les organisations de ce secteur s'expriment dans les premières heures après la crise. Ce secteur est principalement touché par des crises de type « réseau hors service » qui impliquent une réaction rapide. Les secteurs de la grande

distribution et des banques et assurances communiquent plus lentement, entre plusieurs semaines ou mois.

Quelles sont donc les raisons qui poussent une organisation à communiquer tardivement ? Est-ce un refus délibéré de communiquer ? Ont-elles tardé à découvrir le délit ? Quoiqu'il en soit, **lorsqu'une organisation est trop lente pour communiquer, d'autres lanceurs d'alertes prennent le relais.**

1.2. Les canaux de communication

Dans un premier temps, je me suis demandée quel était le canal privilégié par les organisations lors d'une crise de cyberhacking. **La plupart d'entre elles communiquent par le biais d'un communiqué ou d'un article sur leur site web**. Les autres canaux utilisés sont l'e-mailing, les interviews dans les médias et les réseaux sociaux**. Les réseaux sociaux sont rarement utilisés indépendamment d'un autre canal.** Généralement, ils servent de support à la communication principale et « it is about being human and putting personal identity above an instutional identity » (De Pelsmacker, Geuens, Van Den Bergh, 2013, p. 528).

Il semblerait donc que les canaux de communication participent à différents objectifs :

- **Site Web** : publication d'informations officielles comme l'annonce des faits, des mesures mises en place pour éviter que ce scénario ne se reproduise ou encore les modalités d'une éventuelle enquête.
- **Facebook** : publication d'informations moins factuelles, plutôt orientées vers l'aide et l'accompagnement des parties prenantes au travers d'un dialogue ;
- **Twitter** : publication d'informations courtes, factuelles et qui doivent être communiquées le plus rapidement possible.
- **E-mailing** : possibilité d'atteindre directement les potentielles victimes lorsque des données sensibles sont en jeu.

1.3. Le choix de l'ambassadeur

Un autre enjeu de la communication de crise est la tonalité du message et le choix de l'ambassadeur. Je pense que le profil du porte-parole lors d'une crise est implicitement lié à la culture de l'organisation et à la manière dont elle vit cette crise. **La plupart du temps, le choix se porte sur un des métiers en lien avec la communication ou sur l'organisation en son propre nom.**

En réalité, les observations faites lors de l'analyse de cette variable m'ont amenée à un deuxième type de réflexion : quelle importance est attribuée à la sécurité informatique au sein des organisations ?

Le secteur internet est un des seuls secteurs où les experts en sécurité informatique sont les ambassadeurs choisis par les organisations pour communiquer. Dans le contexte actuel, il est difficile de penser que des organisations ne soient pas conscientes de l'enjeu de la protection des données. Dès lors, qu'est-ce que cette observation sous-entend ? Un problème de priorisation, de coûts ou de précipitation ?

1.4. Les stratégies de réponse

Lorsque l'organisation communique, elle opte (de manière consciente ou non) pour une stratégie de réponse. Pour rappel, quatre types de stratégies sont susceptibles d'être mises en œuvre de manière indépendante par l'organisation :

a) La réponse initiale ;
b) La stratégie du déni ;
c) La stratégie du projet latéral ;
d) La stratégie de la reconnaissance.

Le dénominateur commun derrière chaque stratégie est l'attribution de la responsabilité de la crise. **Même si cela n'est pas explicitement présent dans le discours des organisations, chacune se positionne de manière variable en fonction de sa responsabilité face à la crise.**

A. La réponse initiale

La réponse initiale est mise en place dans 99% des cas de cyberhacking. Les deux volets qui la composent se manifestent par le biais de différents discours :

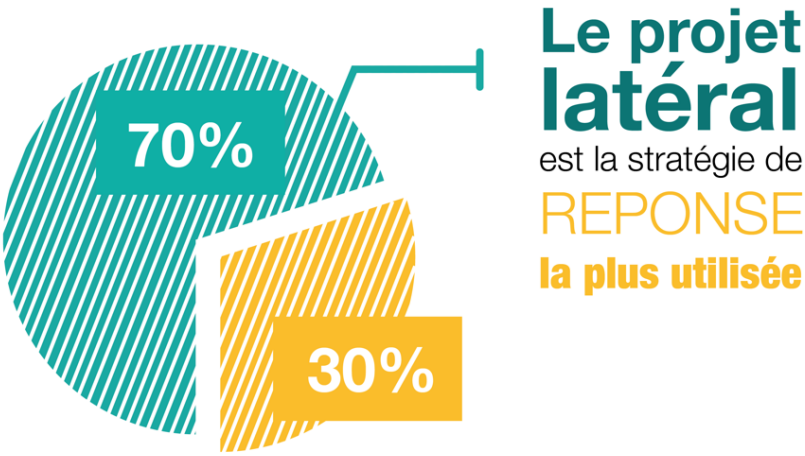
- Les instructions : conseils pour protéger ses données, mises en garde par rapport aux méthodes d'ingénierie sociale ou énumération chronologique des événements ;
- L'adaptation de l'information : rassurer les victimes en leur rappelant que leur confiance est primordiale, collaboration avec des équipes d'experts et les forces de l'ordre dans le cadre d'une enquête.

Certaines organisations (18%) se contentent de cette réponse initiale, comme c'est souvent le cas dans une crise de type « réseau hors service ». Toutes les autres complètent cette réponse de base avec d'autres stratégies de réponse.

B. Le projet latéral

La stratégie la plus utilisée est celle sur projet latéral. Cela signifie que l'organisation ne reconnaît qu'en partie ses responsabilités. Une observation encore plus frappante est la non-utilisation de la stratégie de la reconnaissance.

Figure 8. Le projet latéral, stratégie de réponse la plus utilisée.
N = 97

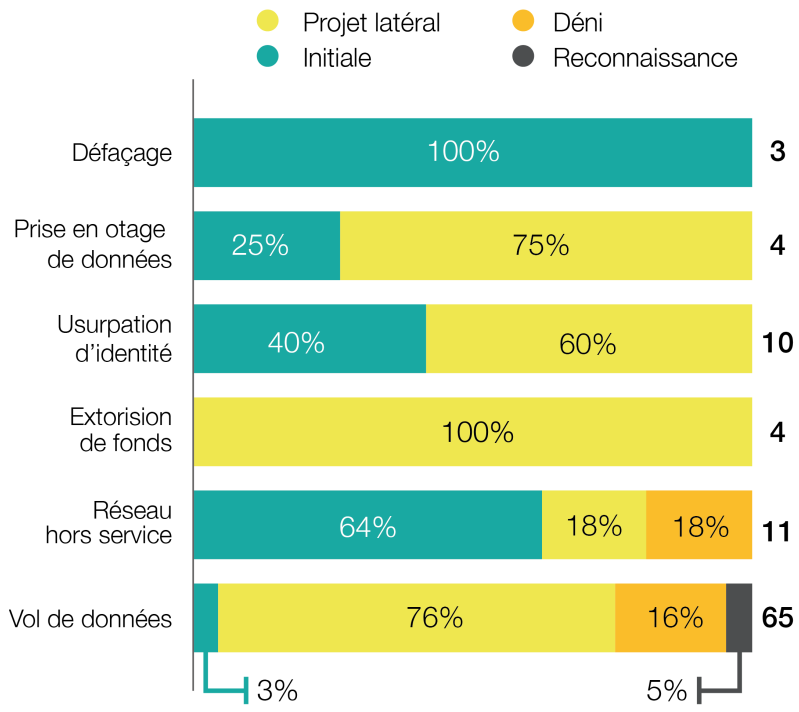


Généralement, l'utilisation de cette stratégie du projet latéral se traduit par le transfert des responsabilités sur le hacker à l'origine du piratage, par l'usage de circonstances atténuantes ou en minimisant les faits. Les organisations privilégient donc l'utilisation de stratégies du projet latéral en accusant le pirate à l'origine du piratage, en se retranchant derrière des circonstances atténuantes et/ou en minimisant les faits.

Le type de cyberhacking et le type de crise selon Coombs influencent le choix de la stratégie du projet latéral.

- Le type de cyberhacking : les organisations qui rencontrent une crise du type « réseau hors service » privilégient, dans un premier temps, la réponse initiale uniquement. Lorsque la crise s'aggrave, elles optent alors pour la stratégie du projet latéral.
- Le type de crise : les organisations qui font face à une crise accidentelle utilisent la stratégie du projet latéral dans 93% du temps, alors qu'une organisation ayant obtenu le statut de victime n'a pas de préférence en matière de stratégie de réponse.

Figure 9. Les stratégies de réponse en fonction du type de cyberhacking.
N = 97



C. La reconstruction

Une stratégie de réponse présente dans ma typologie n'a pas encore été traitée. **Il s'agit de la stratégie de reconstruction, qui n'existe pas indépendamment des autres.** Tout comme les réseaux sociaux viennent en support lors du choix du canal, la reconstruction vient en support aux stratégies de réponse initiale, du déni, du projet latéral et de la reconnaissance.

Figure 10. Le taux d'utilisation de la stratégie de reconstruction.
N = 95

Elle n'est cependant mise en place que dans 30% des cas et accompagnent généralement des stratégies du projet latéral. Cette reconstruction se manifeste au sein des discours des organisations selon trois axes :

- Dédommagement des victimes ;
- Mesures prises pour éviter que la crise ne se reproduise ;
- Bonnes actions faites par le passé.

Le type de crise influence également l'utilisation de la stratégie de reconstruction. Elle est utilisée dans :

- 20% des crises prévisibles ;
- 30% des crises accidentelles ;
- 0% des crises de type victime.

Le résumé du chapitre

Chapitre 5
les points clefs

Les comportements des organisations lors de crises de cyberhacking

Délais de communication

Dans le mois

- Varie avec la **gravité** lors d'un vol
- Secteur le plus rapide : les **médias**
- Si trop lent, réaction d'**autres acteurs**

Ambassadeurs

Métiers de la com ou l'organisation

Secteur internet : experts en sécurité informatique

Canaux de communication

La plupart communiquent par le biais d'un communiqué sur le site web

D'autres canaux, pour d'autres objectifs (Facebook, Twitter, Email)

Stratégies de communication

Réponse initiale 99%

Projet latéral 70%

Reconnaissance 3%

Reconstruction 30%

Le type de cyberhacking et le type de crise selon Coombs influencent le choix de la stratégie.

VI. Conclusion

Il est 8h04 et comme chaque matin depuis plus d'an, une alerte Google programmée à partir de différents mots-clefs liés au cyberhacking arrive dans ma boite mail. Après de nombreuses remises en question sur la thématique, la façon de l'aborder et de la traiter, ce mémoire est l'aboutissement d'une longue réflexion sur la communication de crise lors d'un cyberhacking.

Au début de ma recherche, je m'interrogeais sur la manière dont les organisations malheureusement victimes de ce genre de fraude pouvaient réagir. Mais ce mémoire a pris une direction différente après l'analyse des données. Face à chaque cas, un tout autre genre de question se posait : Et si les crises vécues par les organisations n'étaient pas si imprévisibles ? Et si ces organisations étaient, d'une manière ou d'une autre, aussi responsables de ce qui leur arrive ? Quelles seraient les conséquences sur leur communication ?
Mon angle d'attaque s'est donc déplacé au cours de ma recherche. J'ai d'abord observé les comportements des organisations en tant que victimes de la crise. Ensuite, **j'ai observé ces mêmes comportements communicationnels à travers le prisme de la responsabilité de l'organisation par rapport à la crise.** Ce deuxième regard soulève davantage de questionnements que le précédent.

Les organisations ne manquent pas d'imagination lors de leur communication en temps de crise. De nombreux discours, aussi travaillés soient-ils, se résument finalement par « ce n'est pas ma faute, c'est lui », « il n'y a pas que moi », « oui mais c'est pas si grave », etc. **D'un point de vue sociétal, cette stratégie du projet latéral pose question. Du point de vue de la communication, peut-on réellement reprocher aux organisations de vouloir limiter les dégâts ?** Reconnaître l'entièreté des responsabilités implique de les assumer pendant tout le processus de la crise, cela ne se limite pas à la dimension de la communication. L'aspect juridique rentre également en jeu.

Malgré tout, c'est interpellant de voir **comment ces crises de cyberhacking sont banalisées et rendues légitimes**, comme si chaque organisation devait y passer. En cause aussi, les instituts en sécurité informatique qui alimentent et entretiennent ce fatalisme en publiant des chiffres de plus en plus pessimistes sur le cyberhacking.

Plus surprenant encore, **les responsables en sécurité informatique ne se manifestent presque exclusivement lors de crises concernant des organisations actives dans le secteur internet**, ils prennent rarement la parole dans d'autres secteurs, pourquoi ? Serait-ce une différence de culture et de fonctionnement organisationnels ? La sécurité informatique est un thème (a priori) plus important dans le secteur internet, mais est-il relayé au second plan dans les autres secteurs ?

Autre phénomène marquant, les délais (parfois très longs) entre le piratage et la communication publique des faits. Je trouvais étonnant de la part de ces organisations d'attendre si longtemps avant de communiquer. En fait, la seule solution que j'avais envisagée était la peur de représailles, c'est pourquoi elles optaient pour le silence en espérant que rien ne soit divulgué. Au fur et à mesure de ma réflexion, j'ai compris qu'il ne s'agissait pas plus d'un problème de communication que de sécurité. **Ce n'est pas que les organisations gardent l'information secrète (sauf exception), c'est surtout qu'elles ne savent pas encore qu'elles ont été piratées**. Elles ne le découvrent généralement que lorsqu'une plainte est déposée, que les données sont mises en vente ou qu'un site spécialisé lance l'alerte.

Dans les années à venir, la loi sur la protection des données va se renforcer. Une première directive européenne en matière de protection des données personnelles a vu le jour en 1995. En 2012, un nouveau règlement est apparu, vient d'être approuvé par le Parlement européen et sera d'application dès 2018. Selon cette nouvelle directive, **les organisations qui détiennent des données à caractère personnel sont obligées d'alerter les personnes**

touchées par une fuite de données. Elles doivent également informer les autorités de contrôle en cas de violation importante des données, sans quoi une sanction sera appliquée. Toutes leurs obligations en matière de communication sont reprises dans le règlement général sur la protection des données (GDPR).

Là où cela coince, c'est lorsque le règlement dit « *communicate without undue delay where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person […]* ». À partir de quand considère-t-on qu'il y a un risque important pour les droits et libertés ? Un peu plus bas dans le même article, le règlement s'embrouille. D'abord, l'article dit

- « *without undue delay* »
- « *should be made as soon as reasonably feasible […]* »
- « *not later than 72 hours after become aware of it* »
- « *where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay* ».

Les tentatives de régulation de la communication sont donc bel et bien présentes mais semblent encore devoir évoluer car elles sont sujettes à de multiples interprétations.

Un aspect de la communication que je n'ai volontairement pas abordé est cette dimension d'après-crise. Une fois le bruit autour des événements apaisé, les victimes du piratage sont toujours bien présentes. Il existe donc un deuxième temps de communication. Par exemple, suite au vol de données du site de rencontres extraconjugales Ashley Madison en 2015, des individus ont été la cible de chantage, certains ont démissionné, et des cas de suicides ont été découverts. Alors que l'instant *t* concerne la communication à propos du piratage, l'instant *t+1* se frotte aux conséquences de ce piratage. **Il ne serait donc pas étonnant que dans les prochains mois, voire années, nous entendions parler de certaines conséquences issues de précédents piratages.**

L'important volet numérique développé par les organisations dans la course au *big data* implique de nombreuses adaptations. Récolter et stocker d'immenses quantités de données n'est plus un enjeu de nos jours. **L'enjeu se situe dans d'autres dimensions telles que le traitement de ces données et leur sécurité.** En accordant peu d'importance à l'une ou l'autre de ces dimensions (par manque de temps, d'argent, de ressources ou quoique ce soit d'autre) ou en confondant vitesse et précipitation, les organisations se risquent à des embarras qui auraient pu être évités dans la plupart des cas.
Le paradoxe ? Ce climat de méfiance est pourtant bien ancré dans l'esprit des organisations. Lorsque des organisations « poids lourds » dans leur secteur d'activité comme Yahoo, Target, Sony et d'autres font face à de telles crises de cyberhacking, il est légitime de se poser des questions sur la protection de nos données.

Dans ma définition de la crise, j'insistais sur « *un processus rendu visible par un événement déclencheur (la plupart du temps non prévisible, mais pouvant être anticipé) […]* ». Je pensais que l'événement déclencheur dont je parlais était le piratage et que le processus rendu visible n'était autre qu'un manque de protection informatique. Désormais, je suis plutôt d'avis que ce piratage en tant qu'événement déclencheur reflète un processus plus large que ce simple manque de sécurité**, il s'agit plutôt d'une remise en question des priorités organisationnelles.**

Le comportement des organisations lors de la communication de crise (délai de réaction, choix de l'ambassadeur, stratégies de réponse, etc.) m'amène à penser que le piratage n'est qu'une étape dans le processus de crise, et pas la crise en elle-même.

Je terminerai sur une métaphore, aussi absurde qu'éloquente, qui met le doigt sur une des problématiques développées dans ce mémoire. Elle a été publiée dans un communiqué du groupe de hackers Rex Mundi impliqué dans le piratage des laboratoires Labio en 2015 : « **Ton meilleur ami te prête sa voiture. Tu la gares, au milieu de la nuit, dans un quartier peu sûr, sans**

la verrouiller et avec les clefs à vue sur le siège. De retour le lendemain matin, tu réalises que la voiture n'est plus là, évidemment. Qui est responsable ? Le voleur, bien sûr. Mais et toi, ne l'es-tu pas aussi ? Ton ami te faisait confiance pour garder sa voiture en sécurité, mais tu as échoué. De même, alors que nous sommes manifestement responsables de ces piratages, nous pensons que les organisations ciblées sont également responsables d'avoir laissé les informations de leurs clients être dérobées. Tout ceci crée un dilemme moral très intéressant et fascinant. »[7]

[7] Traduit de l'anglais https://www.databreaches.net/rex-mundi-statement-on-their-motives-and-methods/

Le résumé du chapitre

Bibliographie

Bharat et al. (2016). Anticipatory Cyber Security Research : An Ultimate Technique for the Firts-Move Advantage. *TEM Journal, 5*(1), 3-14.

Bouzon, A. (1999). Communication de crise et maîtrise des risques dans les organisations. *Communication et organisation, 16*. doi : 10.4000/communicationorganisation.2257

Coombs, T., Holladay, S. (2002). Helping crisis managers protect reputational assets. *Management Communication Quarterly, 16*(2), 165)186. doi :10.1177/089331802237233

Coombs, T. (2014). Crisis Management and communications. *Institute for Public Relations*. En ligne http://www.instituteforpr.org/crisis-management-communications/

Coombs, T. (2007). Protecting Organization Reputations During a Crisis : The Development and Application of Situational Crisis Communication Theory. *Corporate Reputation Review, 10*(3), 163-176. En ligne https://lc.cx/SqGG

Conseil de l'Europe. (2004). *Convention on Cybercrime*, Budapest. En ligne http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_fr.pdf

De Perlsmacker, P., Gueuens, M., Van Den Bergh, J. (2013). *Marketing Communications : A European Perspective* (5e éd.). Pearson.

European Cybercrime Center. (2014). *First year report*. En ligne https://www.europol.europa.eu/publications-documents/european-cybercrime-center-ec3-first-year-report

Frandsen, F., Johansen, W. (2007, mai). *Communication and the Rhetorical Arena : A Multivocal Approach*. Communication présentée au congrès annuel de l'Internaiton Communication Association, San Fransisco.

Résumé repéré à http://citation.allacademic.com/meta/p171526_index.html

Frandsen, F., Johansen, W. (2017). *Organizational Crisis Communication – A Multivocal Approach*. SAGE Publishing.

Heiderich, D. (2008). La gestion de crise a un demi-siècle. *Magazine de la communication de crise et sensible*. En ligne http://www.communication-sensible.com/download/La-gestion-de-crise-a-un-demi-siecle.pdf

Heiderich, D. (2010). *Plan de gestion de crise*. Dunod.

Lagadec, P. (1999). Communication de crise, communication en crise. *Risque et Société*, 197-207. En ligne http://www.patricklagadec.net/fr/pdf/Communication.pdf

Leman-Langlois, S. (2006). Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberespace commercial. *Criminologie*, *39*, 63-81. doi :10.7202/013126ar

Lagadec, P. (1991). *La gestion des crises : outils de réflexion à l'usage des décideurs*. Ediscience international. En ligne http://www.patricklagadec.net/fr/pdf/integral_livre1.pdf

Leplat, J. (2002). De l'étude de cas à l'analyse de l'activité. *Perspectives interdisciplinaires sur le travail et la santé, 4*(3). doi : 10.4000/pistes.3658

Libaert, T. (2015). *La communication de crise* (4e éd.). Parid : Dunod.

Règlement (UE) du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). En ligne http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR