Les techniques de gestion des risques, à l’ère de la digitalisation

Présentée par: M. Adlane HAFFAR

Logique de présentation

1. Introduction
2. Identification des sources de risque
3. Atteintes aux données
4. Atteintes aux systèmes d'information
5. Techniques de gestion des cyber-risques
6. Conclusion

Introduction (1/7)

Préambule:

Quelle que soit son activité ou sa taille, chaque entreprise doit prendre conscience de son exposition aux cyber-risques.

Ce risque étant en progression constante, il est impératif aujourd’hui que l’entreprise mette en place une gestion des risques performante et les outils nécessaires pour se prémunir d’une cyber-attaque.

Introduction (2/7)

Le choix s’est porté sur cette thématique pour les raisons suivantes:

De nos jours, presque toutes les entreprises disposent d’un système d’information.

De plus en plus d’entreprises Algériennes sont séduites par le recours à la digitalisation.

On constate également une professionnalisation des pirates informatiques.

Introduction (3/7)

Notre objectif est triple:

Sensibiliser les opérateurs économiques sur les cyber-risques.

Exposer quelques retours d’expérience de multinationales.

Discuter des différentes solutions de protection qui existent à travers le monde.

Introduction (4/7)

Qu’il soit interne ou externe, nous pouvons illustrer un réseau informatique de la façon suivante:

Introduction (5/7)

Quelques idées reçues:

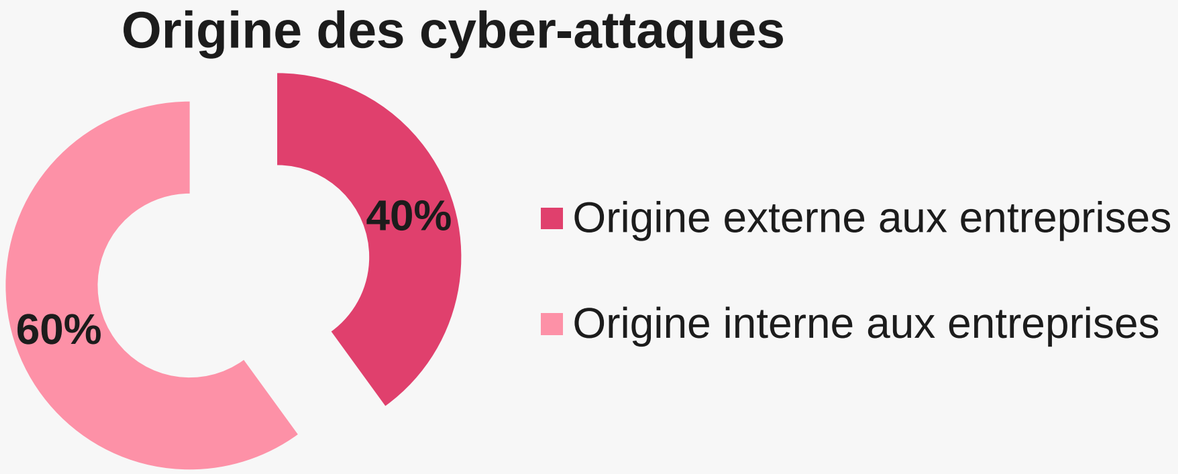
Je suis une PME/PMI, donc je ne suis pas concernée par les cyber-risques.

Ne se considérant pas comme une cible, la PME/PMI est le moyen idéal pour les pirates informatiques d’introduire le système d’information d’un grand groupe.

Introduction (6/7)

Quelques idées reçues:

Je ne suis pas une entreprise connectée, donc je ne suis pas exposée aux cyber-attaques.



Source: IBM, Cyber Security Intelligence Index 2016.

Introduction (7/7)

Quelques idées reçues:

Dans mon contrat d’assurance, j’ai la garantie « Tous Risques Informatiques », donc je suis couvert.

La garantie « Tous Risques Informatiques » couvre uniquement les pertes physiques (dommages aux matériels) et les pertes de données.

Identification des sources de risque (1/6)

La dépendance à l'informatique:

Les connexions sans fil.

Les réseaux informatiques.

L'e-commerce.

Les systèmes informatiques industriels.

Identification des sources de risque (2/6)

Cas N°1: Affaire Renault/Nissan

Du vendredi 12 au samedi 13 Mai 2017, un nombre important de sites du constructeur Renault ont été infectés par un virus informatique, et le problème s'est étendu à sa filiale Nissan, dont l'usine géante de Sunderland a dû, elle aussi, stopper sa production.

Conséquence: arrêt de la production durant 3 jours.

Identification des sources de risque (3/6)

Le facteur humain:

La collecte de données des salariés.

Usage par les salariés de l’outil informatique.

Usage des périphériques personnel à des fins professionnelles.

Identification des sources de risque (4/6)

Cas N°2:

Une DRH d’un grand groupe international a vu son ordinateur dérobé dans un train et dans lequel figurait le fichier du personnel de l’ensemble des filiales du groupe.

Conséquence: notification à chaque salarié du groupe afin de les informer du vol des données personnelles.

Identification des sources de risque (5/6)

La sous-traitance:

Le Cloud Computing: est un mode de traitement des données d’un client, dont l’exploitation s’effectue par internet, sous la forme de services fournis par un prestataire.

Les Data Centers: est une solution d’hébergement des données, mais aussi des serveurs.

Le Big Data: qui recoupent le traitement d’une volumétrie très importante de données.

Identification des sources de risque (6/6)

Cas N°3: Affaire UMP contre Oracle

Le 30 décembre 2010, l'UMP a conclu avec la société Oracle France une prestation de gestion et d'hébergement des données de l'UMP (Cloud Computing).

Le 29 Décembre 2012, l'UMP souhaitant récupérer ses données, a sollicité Oracle France, qui n'a pas pu les restituer à cause d'un « bug ».

Conséquence: condamnation d'Oracle France à une amande de 5 000 € par jours de retard, jusqu'à restitution des données.

Atteintes aux données (1/4)

Définition:

On parle d’atteinte aux données lorsqu’un incident a pour conséquence la violation de la confidentialité des données, qu’elles soient à caractère personnel ou confidentiel.

Atteintes aux données (2/4)

Les cas classiques d'atteinte aux données sont les suivants:

Vol ou perte de PC portable, disque dur externe, clé USB, CD Rom.

Divulgation d'informations sur les réseaux sociaux.

Vol ou perte de données par un sous-traitant qui utilise les données pour l'exercice de sa prestation.

Atteintes aux données (3/4)

Voici repris dans un tableau les cas les plus médiatisés d'atteintes aux données:

Nombre de données concernées	Date de l'atteinte aux données	Identité de la société	Secteur d'activité
56 000 000	Août 2014	Home Depot	Grande distribution
152 000 000	Octobre 2013	Adobe	Informatique
145 000 000	Mai 2013	eBay Inc	Payement en ligne
110 000 000	Décembre 2013	Target	Grande distribution
130 000 000	Janvier 2009	Heartland Payment Systems	Paiement par carte bancaire
94 000 000	Janvier 2007	TJX Companies Inc	Grande distribution

Source: Zicry Laura (2014). « Enjeux et maîtrise des cyber-risques ». Éditions L'ARGUS de l'assurance. France. Page N°54.

Atteintes aux données (4/4)

À la suite d'une atteinte aux données, les conséquences pour l'entreprise sont les suivantes:

Frais de reconstitution des données.

Dépenses de relations publiques.

Frais de notification aux autorités administratives et coût de la communication aux personnes concernées.

Responsabilité civile liée à la protection des données personnelles.

Honoraires d'avocat, d'experts ou de consultants.

Responsabilité civile de l'entreprise engagée du fait de la transmission d'un virus informatique dont l'entreprise a elle-même été victime.

Atteintes aux systèmes d’information (1/6)

Définition:

L’atteinte aux systèmes d’information peut se matérialiser de différentes façons:

Accès à un système d’information sans y être autorisé est déjà considéré comme une atteinte.

Rendre indisponible l’accès à un système d’information ou à un site web (attaque par déni de service).

Introduction d’un logiciel malveillant dans le but d’infecter un système d’information.

Atteintes aux systèmes d’information (2/6)

Définition:

Envoi de faux mails qui contiennent un logiciel malveillant qui va infecter un ordinateur et crypter certains fichiers, une rançon est alors demandée pour obtenir la clé permettant de décrypter les données (Rançongiciel).

Introduction du pirate dans le système d’information, afin de crypter des fichiers clés de l’entreprise, et de demander ensuite le paiement d’une rançon sous la menace de divulguer à la fois l’attaque mais aussi le vol de données (Cyber-extorsion).

Atteintes aux systèmes d’information (3/6)

À la suite d’une atteinte aux systèmes d’information, les conséquences pour l’entreprise sont les suivantes:

Honoraires d’une société spécialisée afin de conserver, collecter et analyser les preuves numériques de l’atteinte, en vue de les produire dans le cadre d’une action en justice.

Frais et coût afin de retrouver une situation normale et remettre l’entreprise dans l’état où elle se trouvait avant l’attaque.

Frais visant à décontaminer soit le système d’information, soit les matériels.

Atteintes aux systèmes d’information (4/6)

À la suite d’une atteinte aux systèmes d’information, les conséquences pour l’entreprise sont les suivantes:

Honoraires d’entreprises spécialisées dans le décryptage de données.

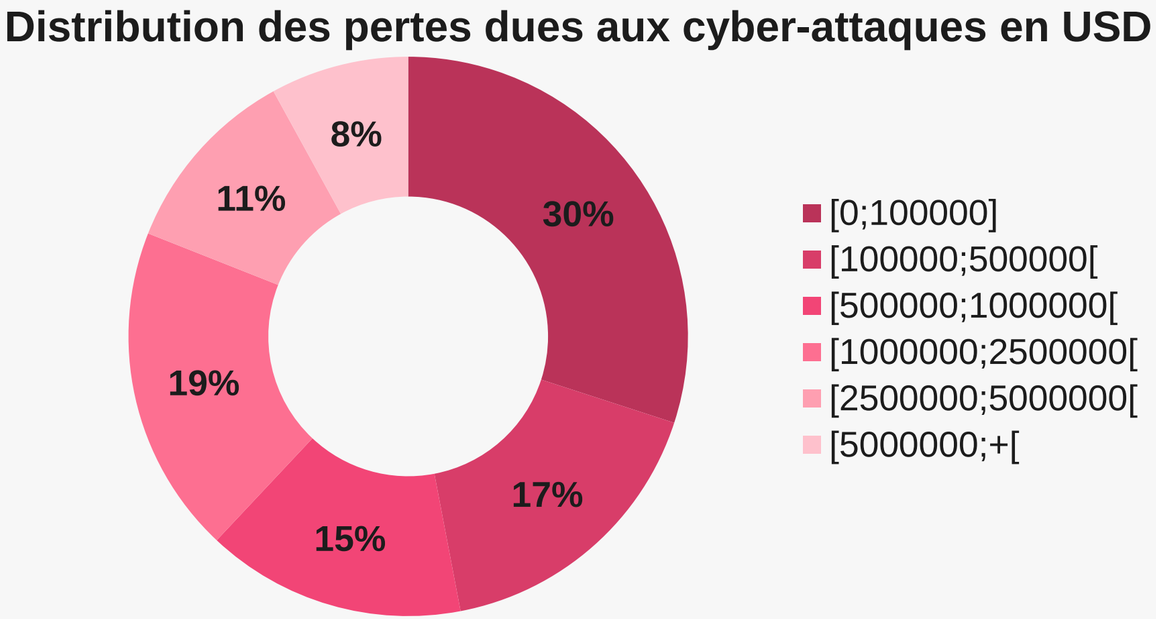
Frais supplémentaires d’exploitation (Location de nouveaux locaux, recours à une société d’intérim…).

Pertes d’exploitation (arrêt de la production, pénalité de retard, baisse du chiffre d’affaires…).

Dépenses de relations publiques qui visent à informer mais aussi à dédramatiser l’événement.

Atteintes aux systèmes d’information (5/6)

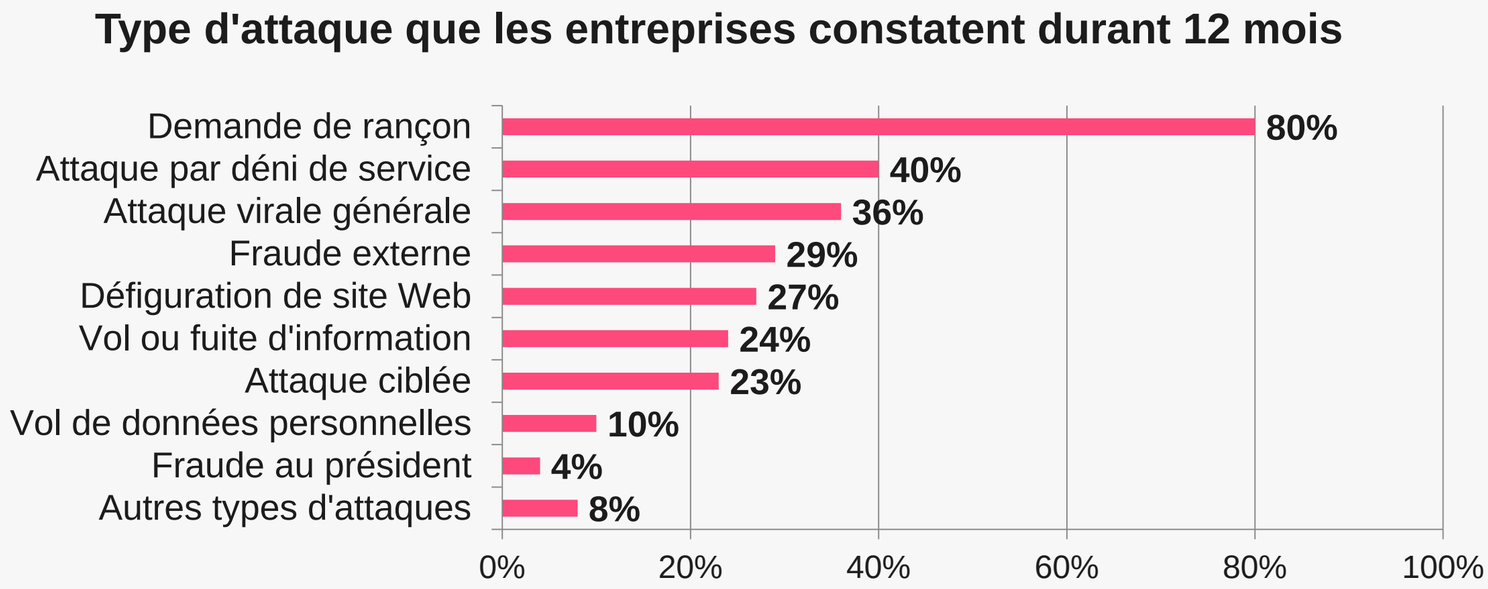
Quelque statistiques:



Source: CISCO 2018 Security Capabilities Benchmark Study.

Atteintes aux systèmes d’information (6/6)

Quelque statistiques:



Source: Enquête opinionway réalisée auprès de 141 membres du CESIN.

Techniques de gestion des cyber-risques (1/14)

Pour se couvrir contre les cyber-risques, l'entreprise dispose de trois niveaux de protection:

Le premier niveau de protection est évidemment la loi, qui condamne et punit les responsables des cyber-attaques.

En Algérie, la Loi N°18/04 du 24 Chaâbane 1439 correspondant au 10 mai 2018 a été promulguée, afin de fixer les règles générales relatives à la poste et aux communications électroniques.

Techniques de gestion des cyber-risques (2/14)

Pour se couvrir contre les cyber-risques, l'entreprise dispose de trois niveaux de protection:

Le deuxième niveau de protection, consiste à moderniser les moyens de prévention, notamment les points suivants:

Créer la fonction « Responsable de la Sécurité des Systèmes d'Information ».

Mettre en place une cartographie des risques.

Mettre en place une charte informatique.

Prévoir une politique de gestion des mots de passe.

Prévoir un plan de reprise/continuité de l'activité.

Mettre en place une cellule de veille.

Techniques de gestion des cyber-risques (3/14)

Pour se couvrir contre les cyber-risques, l'entreprise dispose de trois niveaux de protection:

Le premier et deuxième niveau de protection permettent de réduire considérablement les cyber-risques, mais pas de les éliminer complètement, c'est pour cette raison que l'entreprise recours à un troisième niveau de protection, à savoir transférer les cyber-risques à l'assurance.

Techniques de gestion des cyber-risques (4/14)

Pour se couvrir contre les cyber-risques, l'entreprise dispose de trois niveaux de protection:

Les contrats d'assurance de responsabilité civile et de dommages aux biens ont vocation à garantir des dommages. Ceux-ci sont causés soit à:

Un tiers, on parle alors de responsabilité civile si l'on peut reconnaître une faute à l'origine d'un dommage, et un lien de causalité entre la faute et le dommage.

L'assuré lui-même, on parle alors d'assurance de dommages qui a vocation à garantir les dommages causés aux biens de l'assuré et/ou les pertes d'exploitation.

Techniques de gestion des cyber-risques (5/14)

Dans les contrats de responsabilité civile, on distingue 4 catégories de dommages, qui sont repris dans le tableau ci-dessous:

Type de dommage	Description
Dommage corporel	Tout atteinte à l'intégrité physique ou morale subie par tout être humain.
Dommage matériel	Toute détérioration, altération, destruction ou perte d'une chose ou substance.
Dommage immatériel consécutif	Tout préjudice pécuniaire, autre qu'un dommage corporel ou matériel, qui est consécutif à un dommage corporel ou un dommage matériel.
Dommage immatériel non consécutif	Tout préjudice pécuniaire, autre qu'un dommage corporel ou matériel, qui n'est pas consécutif à un dommage corporel ou un dommage matériel.

Techniques de gestion des cyber-risques (6/14)

Généralement, un sinistre cyber crée un dommage immatériel non consécutif.

En effet, un virus, une attaque par déni de service ou une demande de rançon suite à une intrusion dans un système d'information ne crée aucun dommage corporel ni matériel.

Beaucoup d'assurés ont tendance à penser qu'ils sont couverts lorsqu'ils bénéficient de la garantie de responsabilité civile et de dommage aux biens.

Ils pensent que cette garantie couvre les dommages immatériels non consécutifs et les pertes d'exploitation qui en résultent, mais la réalité est toute autre.

Techniques de gestion des cyber-risques (7/14)

Le recours à un conseiller en assurance devient central.

Une analyse approfondie et technique des contrats d’assurance est donc non seulement nécessaire mais également indispensable pour avoir une bonne vision de ses couvertures assurantielles, et de s’assurer qu’aucune exclusion ne viendrait réduire le champ d’application du contrat d’assurance.

Techniques de gestion des cyber-risques (8/14)

Cas N°4: Affaire Sony

En 2011, un hacker avait piraté le système d'exploitation de la Playstation, en bloquant l'accès à son site web, et en volant les données des joueurs.

Les frais et coûts engagés par la société Nippone ont atteint des records (On parle de 177 millions $), incluant les frais d'avocat, de notification aux autorités nationales et aux personnes concernées, et les amendes qui ont été prononcées à l'encontre de l'entreprise.

Techniques de gestion des cyber-risques (9/14)

Cas N°4: Affaire Sony

Le cours de l'action Sony à la bourse a énormément chuté pour descendre jusqu'à 13 dollars alors qu'il atteignait plus de 30 dollars avant les révélations.

C'est tout naturellement vers son assureur de responsabilité civile que Sony s'est retourné, pour obtenir la prise en charge des frais relatifs à l'atteinte à la vie privée, dont ont été victimes les joueurs de Sony, du fait de la divulgation de leurs données personnelles.

Techniques de gestion des cyber-risques (10/14)

Cas N°4: Affaire Sony

L’assureur a décidé de saisir la justice afin de faire reconnaitre que la garantie n’était pas due et qu’il n’avait aucune obligation contractuelle de défendre Sony.

Le juge a décidé que les conditions de mise en jeu de la garantie n’étaient pas réunies. En effet, le contrat d’assurance prévoyait que la garantie était due si la divulgation d’éléments qu’ils soient oral ou écrit, était le fait de l’assuré.

Techniques de gestion des cyber-risques (11/14)

Cas N°4: Affaire Sony

Or, dans le cas présent, la divulgation des données personnelles n’est pas le fait de Sony mais du hacker qui a divulgué les informations confidentielles appartenant à des millions de joueurs.

Le contrat d’assurance souscrit par Sony couvre la faute commise par Sony lui-même et requiert donc que ce soit l’assuré qui commette cette faute. Or, dans ce cas de figure, tel n’était pas le cas.

Techniques de gestion des cyber-risques (12/14)

Pour les entreprises qui souhaitent se couvrir contre les cyber-risques, il existe deux solutions d'assurance possibles:

Étendre les garanties des contrats traditionnels en y intégrant les couvertures cyber.

Souscrire un contrat cyber en « *stand-alone* », c'est-à-dire un contrat spécifique indépendant des autres garanties.

Techniques de gestion des cyber-risques (13/14)

Le tableau ci-dessous, indique les garanties offertes, pour l'assurance responsabilité civile.

Couvertures de la responsabilité civile	Contrat
Frais de défenses et conséquences pécuniaires liée à la protection des données personnelles/confidentielles	**Responsabilité Civile au titre de la protection des données personnelles et confidentielles (spécial)**
Frais de défenses et conséquences pécuniaires liée à la sécurité des systèmes d'information	**Responsabilité Civile au titre d'une atteinte au système d'information (spécial)**
Conséquences de la transmission de virus informatique subies par l'assuré	Responsabilité Civile (traditionnel)
Frais d'enquête, d'assistance et représentation devant des autorités administratives	Responsabilité Civile (traditionnel)

Techniques de gestion des cyber-risques (14/14)

Le tableau ci-dessous, indique les garanties offertes, pour les assurances dommage et perte d'exploitation.

Couvertures des dommages et pertes d'exploitation	Contrat
Frais de reconstitution de données	Dommage Tous Risques Informatiques (traditionnel)
Frais supplémentaires d'exploitation	**Fraude (spécial)**
Pertes d'exploitation	**Frais supplémentaires d'exploitation et pertes d'exploitation (spécial)**
Frais de gestion de crise/dépenses de relations publiques	**Frais de relations publiques à la suite d'un événement médiatique (Spécial)**
Extorsion de fonds	**Kidnap and Ransom/Cyber-extorsion (spéciaux)**
Frais de notification aux autorités administratives et aux Tiers	**Frais de notification et de communication (spécial)**
Frais de décontamination des systèmes informatiques	**Fraude (spécial)**
Honoraires d'expert	**Fraude/Frais de remédiation (spéciaux)**

Conclusion (1/1)

L’adage dit:

Un homme averti en vaux deux.

Une entreprise bien assurée en vaux combien ?

Merci pour votre aimable attention

LOGISTICAL 2018

• • •