Cahiers Techniques 2015

Commission
Systèmes d'Information

CYBER RISQUES

Outil d'aide à l'analyse et au traitement assurantiel

En partenariat avec le CESIN

AMRAE
L'ASSOCIATION

A propos de l'AMRAE

L'Association pour le Management des Risques et des Assurances de l'Entreprise rassemble plus de 900 membres appartenant à 550 entreprises françaises publiques et privées.

L'association a notamment pour objectifs de développer la « culture » du Management des Risques dans les organisations et d'aider ses membres dans leurs relations avec les acteurs du monde de l'assurance et les pouvoirs publics. Elle les conseille dans l'appréciation des risques, dans la maîtrise de leurs financements et leurs dépenses d'assurance.

Sa filiale AMRAE Formation, pour répondre aux besoins de formation professionnelle de ses adhérents ou de ceux qui légitimement s'adressent à elle, dispense des formations diplômantes, certifiantes et qualifiantes de haut niveau.

A propos du CESIN

Le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) est une association loi 1901, créée en juillet 2012, avec des objectifs de professionnalisation, de promotion et de partage autour de la Sécurité de l'Information et du Numérique.

Le CESIN est un lieu d'échange de connaissances et d'expériences qui permet la coopération entre experts de la Sécurité de l'Information et du Numérique et entre ces experts et les pouvoirs publics.

Le Club conduit des ateliers et groupes de travail, mène des actions de sensibilisation et de conseil, organise des congrès, colloques ou conférences.

Il participe à des démarches nationales dont l'objet est la promotion de la Sécurité de l'Information et du Numérique. Il est force de proposition sur des textes règlementaires, guides et autres référentiels.

Le CESIN réunit environ deux cents membres issus de tous secteurs d'activité :
des membres actifs, responsables de la sécurité de l'information dans leur organisation, des membres associés, représentants de diverses autorités en charge de la Sécurité de l'Information au plan national, des juristes experts de la sécurité des TIC (Technologies de l'Information et des Communications).

L'AMRAE adresse ses remerciements à ceux qui ont contribué à la réalisation de cette publication

L'AMRAE tient à remercier tous les membres du Groupe de travail « Cyber assurance » de la Commission Systèmes d'Information de l'AMRAE, Risk Managers issus de différents secteurs (Banque, Industrie et Services …), ainsi que les membres du CESIN qui ont participé à la constitution de cet outil et plus particulièrement :

- François Beaume, Président de la Commission SI de l'AMRAE, Deputy Group Risk Manager and Insurance Director, Bureau Veritas

- Alain Bouillé, Président du CESIN

- Hélène Dubillot, Directrice Coordination Scientifique, AMRAE

- Fabrice Morgaut, Insurance and Risk Manager, Transdev

- Pascal Richard, Responsable des Assurances Non-Vie, Société Générale

L'AMRAE tient à remercier les courtiers ayant permis une actualisation de l'état du marché en Annexe 2 du présent document.

Table des matières

Editorial

Chers Membres de l'Amrae,

Le sujet des risques numériques est depuis quelques années de plus en plus prégnant : pas une semaine ne se passe sans qu'une illustration concrète de sa réalité ne défraie la chronique.

Au-delà de l'impact opérationnel, de récentes actualités ont souligné que, suite à des attaques cybercriminelles, **certains dirigeants et administrateurs ont vu leur responsabilité être mise en cause, ainsi que celle de leur entreprise**. Pour d'autres entreprises, ce type de risque a provoqué, à terme, **leur faillite pure et simple.**

Ces risques mettent à mal les frontières existant jusqu'alors : le Système d'Information de l'Entreprise et les données qu'il véhicule sont de plus en plus fréquemment externalisés dans le Cloud au moyen d'une chaîne de prestataires, mixant les cotraitants et sous-traitants extérieurs à l'entreprise, abolissant ainsi les frontières physiques et géographiques et complexifiant le partage des responsabilités. Cette transformation en profondeur du Système d'Information de l'Entreprise et les nouveaux usages qui en découlent ont fait naître de nouveaux risques, ceux-là même que l'on qualifie aujourd'hui de « Cyber risques ».

Cette transformation génère, notamment pour le Risk Manager, une complexité supplémentaire à prendre en compte dans les analyses de risques qu'il réalise avec les métiers. Complexité dont il doit comprendre les arcanes par une proximité avec les différents acteurs en charge : Directeur des Systèmes d'Information (DSI), Directeur de la Sécurité de l'information (CISO), Correspondant Informatique et Libertés (CIL), …

La couverture de ces risques, d'une nature différente de risques plus traditionnels (risques de dommages ou de responsabilités), entraine une nécessaire adaptation de l'industrie de l'assurance. Leur traitement, qui aujourd'hui semble vouloir se réaliser par le truchement de couvertures dédiées regroupées sous le terme de « Cyber assurance », nécessite également de redéfinir les frontières des branches d'assurance existantes.

Forte de ces constats, l'AMRAE, au travers de sa Commission Systèmes d'Information, a, début 2014, constitué un Groupe de Travail conjoint avec le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique), afin de définir une méthodologie et de constituer **un outil utile et pratique, capable d'aider le Risk Manager et les différents acteurs du SI à :**

- identifier et évaluer les risques « cyber », en fonction de son univers propre de cyber risques,

- mettre en évidence les moyens de réduction déjà en place,
- analyser les réponses apportées par les programmes d'assurance en place,
- définir les éventuels besoins de couvertures d'assurance « cyber » complémentaires.

C'est le résultat de ces travaux que nous vous livrons dans ce nouveau Cahier Technique, complété d'une mise à jour de l'Etat du Marché pour cette branche d'assurance.

Nous espérons que vous trouverez cet outil utile et nous restons à votre disposition pour parler de vos retours d'expérience à ce sujet, et continuer à enrichir éventuellement la méthodologie proposée.

François Beaume
Président de la Commission Systèmes d'Information AMRAE

Objectifs et méthodologie

Mis en place début 2014, au sein de la Commission Systèmes d'Information de l'AMRAE, le Groupe de Travail « Cyber Assurance » regroupe des Risk Managers issus d'entreprises de différents secteurs (Banque, Industrie, Services, Hi-Tech …) ainsi qu'un RSSI membre du CESIN, Club des experts de la sécurité de l'information et du numérique.

Ce Groupe de Travail avait pour objectif principal de **définir les besoins génériques des entreprises en matière d'assurance Cyber.** Cet exercice a été réalisé, d'abord sous la forme d'un partage d'expériences entre ses membres, complété ensuite d'une enquête auprès de courtiers partenaires de l'AMRAE, sur leur compréhension :

- du cyber risque,

- des besoins des entreprises en matière de cyber assurance,

- et de manière plus générale, du marché de l'assurance cyber.

Les éléments recueillis ont permis de réaliser **une « matrice type » d'analyse des cyber risques et des couvertures d'assurance en place au sein d'une entreprise**, première étape nécessaire pour, ensuite, qualifier le besoin ou non de souscription d'une couverture cyber dédiée, et en définir plus précisément les contours.

Le caractère pluridisciplinaire, ou transverse, de cette analyse, **qui doit impliquer la fonction Management des Risques comme la fonction Systèmes d'Information dans leurs diverses dimensions,** la rend complexe à réaliser. Cette première étape vise à identifier les risques propres à cette thématique Cyber, à en quantifier les impacts, et à décrire les moyens de réduction du risque déjà en vigueur.

Sur la base de cette première analyse, il convient ensuite de voir avec les métiers impactés quelles mesures de prévention complémentaires peuvent être mises en œuvre pour, si possible, réduire le risque, que ce soit dans sa fréquence de réalisation ou dans son intensité.

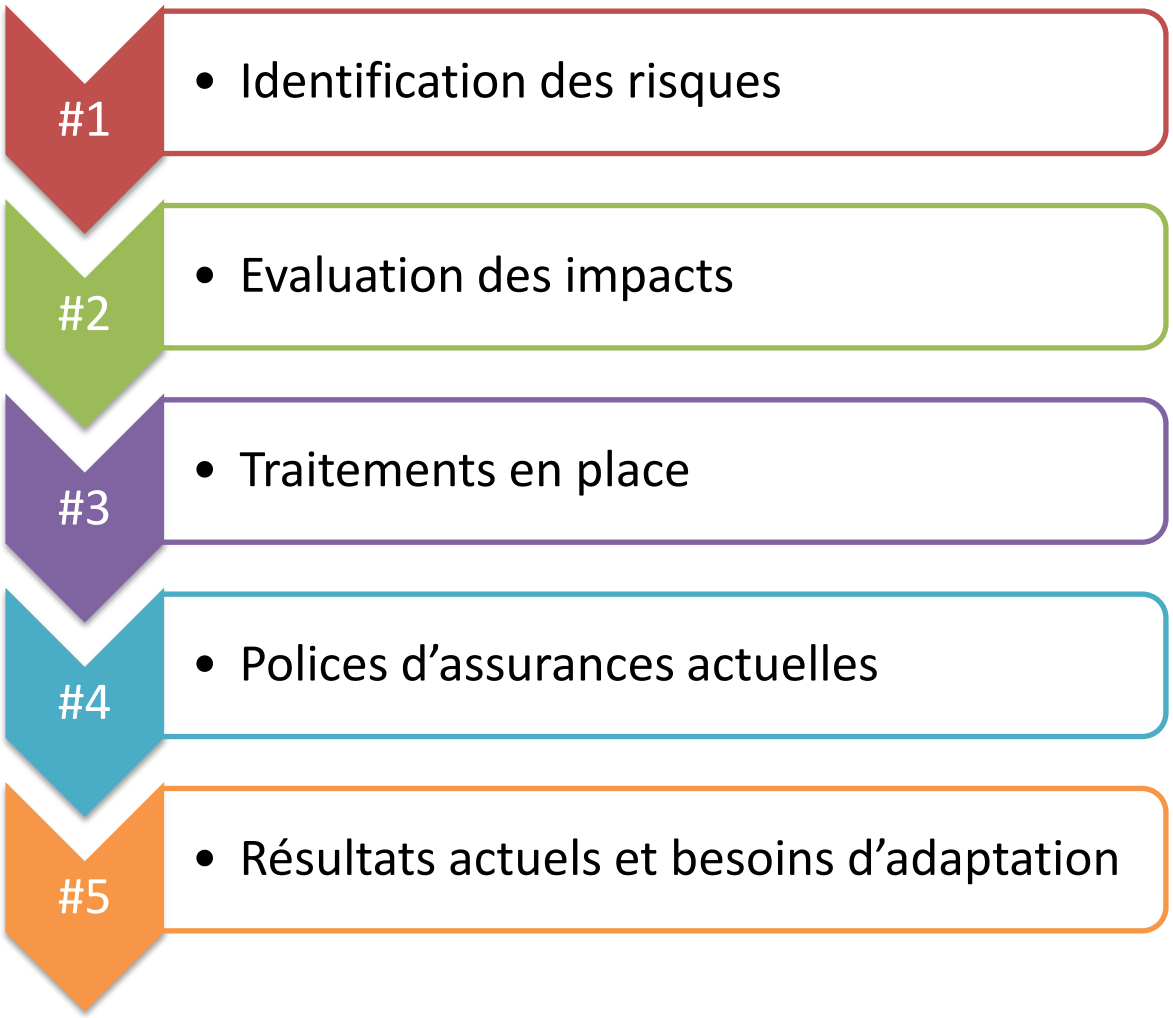
Toujours sur la base de cette première analyse, il va être ensuite possible de définir quelles garanties les contrats d'assurance existants (Dommages, RC …) peuvent apporter, et de déterminer les besoins en couverture complémentaire potentiellement assumables par une police dédiée « Cyber ».

Matrice d'analyse des risques « cyber »

Les travaux du groupe de travail ont débouché sur la matrice Excel disponible en annexe de ce Cahier Technique.

Cette matrice a pour vocation d'être un outil de travail au service du Risk Manager, lui permettant de poser les bases d'une analyse précise de l'univers des risques cyber de son entreprise. L'AMRAE met à disposition cet outil EXCEL pour ses membres dans la section Commission Systèmes d'Information de son espace membre.

La matrice proposée est structurée autour de 5 étapes clefs :



L'étape #1 : Identification des risques

Elle se matérialise dans la matrice par la description précise d'**une liste indicative de scenario de risques « Cyber »**, à laquelle l'entreprise du Risk Manager est susceptible d'être exposée. Cette liste, fruit des échanges du groupe de travail, doit bien évidemment être personnalisée, amendée ou complétée, en fonction de l'univers de risque propre à chaque entreprise, ses métiers et les territoires où elle réalise ses activités.
Chaque risque doit être objectivé pour être compréhensible de manière identique par les différents acteurs impliqués dans l'analyse.

Pour comprendre au mieux les scenarii de risques proposés, nous recommandons que chaque terme utilisé soit expliqué et partagé entre les métiers SI et Risk Management via un vocable commun. Les échanges du groupe de travail ont en effet montré combien il est important d'arriver à une lecture et une compréhension commune de chaque terme employé, afin de partager le scénario.

L'étape #2 : Evaluation des impacts

Elle vise à lister **les typologies d'impacts** de chacun des risques. Cette description des impacts est scindée en deux :

- impacts sur l'assuré (ie. l'entité objet de l'étude),

- impacts sur les tiers.

Cette description sera ensuite complétée par une **évaluation financière** des typologies d' impacts identifiés.

L'étape #3 : Traitements en place

Cette étape s'intéresse aux mesures de gestion et de réduction des risques déjà en place et/ou jugées nécessaires et demande de les décrire.

Cette étape n'est pas présente dans la matrice dans sa version actuelle mais pourrait facilement être ajoutée sous la forme d'une colonne supplémentaire.

Il s'agit essentiellement de lister **les mesures de prévention et ou protection** mises en place dans l'entreprise. Ceci permet « d'affiner » l'analyse de l'intensité de l'impact, de passer à la quantification d'un impact des risques résiduels, puis de faire le lien avec la couverture assurantielle actuelle décrite en étape #4.

L'étape #4 : Polices d'assurances actuelles

Elle permet au Risk Manager de décrire la ou les réponses apportées par les polices d'assurance en place au sein de l'organisation. Les polices qui doivent être décrites ici sont par exemple les polices :

- Dommages aux Biens et/ou Pertes Financières Consécutives,
- Responsabilité Civile Générale,
- Fraude,
- Autres types (à décrire selon l'entreprise objet de l'analyse),
- Cyber
- …

Cette étape se réalise par une description, par risque identifié et pour chaque police listée :

- des frais et postes de dépenses couverts,
- des frais qui ne seraient pas couverts par ces polices mais qui pourraient l'être en étendant une garantie,
- des niveaux « idéaux » de garantie,
- des limites des programmes actuels.

L'étape #5 : Résultats actuels et besoins d'adaptation

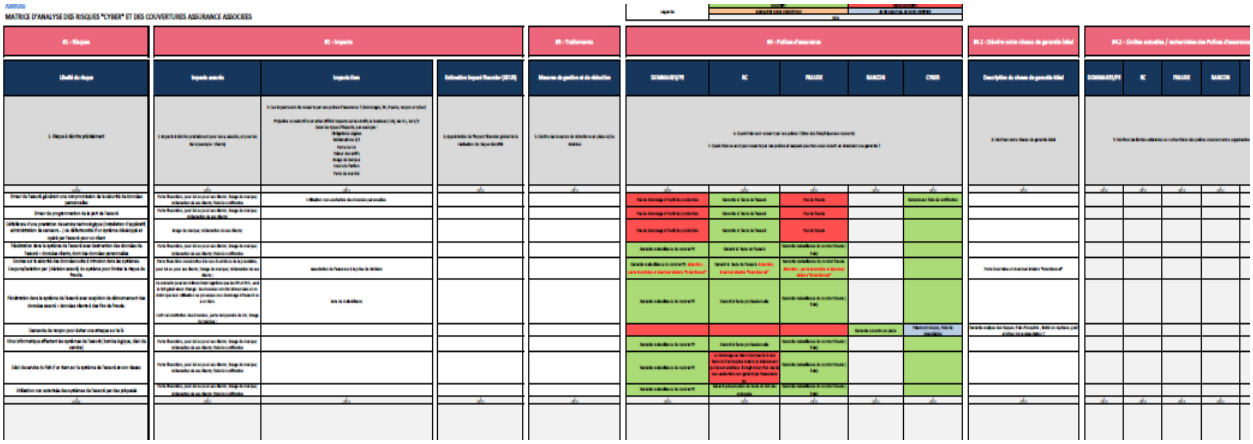
Non formalisée dans la matrice Excel, cette étape est la synthèse de l'analyse. Cette synthèse permet le questionnement de l'efficacité des solutions de traitement et de financement en place : ce système est-il adapté et aussi efficace que prévu ?

La réponse à ces questions peut, le cas échéant, déboucher sur la définition d'un ou plusieurs plans d'action, que ce soit pour compléter ou faire évoluer des mesures de gestion ou de réduction du risque, pour ajuster les garanties et limites des polices en place, ou pour soucrire une garantie dédiée « Cyber » dont les contours seront définis par le résultat de l'analyse décrite plus avant.

Conclusion

Les étapes qui sont décrites précédemment constituent les étapes clés de la matrice EXCEL, crée par le groupe de travail, pour permettre aux Risk Managers de mieux analyser leur besoin.

Cette matrice (photo ci-dessous) est présentée dans l'annexe 1 sous la forme d'un fac similé. La matrice elle-même est, pour les membres AMRAE, téléchargeable, dans la section Commission Systèmes d'informations de l'espace membre de son site web.



Le sujet du traitement assurantiel des cyber risques évolue aussi vite que les cyber risques eux-mêmes, pour preuve l'accroissement rapide de la capacité disponible sur ce marché. De ce fait, les travaux du groupe de travail vont se poursuivre, ne serait-ce que pour pérenniser l'outil présenté ici et lui permettre de rester actuel.

De nombreuses autres questions restent par ailleurs à traiter, que ce soit sur le volet de la mise en œuvre de polices Cyber au sein de groupes multinationaux, la structuration même des polices Cyber pour qu'elles répondent aux besoins des Risk Managers, l'éventuelle implication de captives de réassurance dans la souscription de risques cyber (seules 1% des captives existantes souscrivent des risques Cyber – source Aon Global Risk Consulting's 2014 Captive Benchmarking tools)...

Annexe 1 : Matrice

Un fac-similé de la matrice Excel est présenté dans les pages suivantes.

La matrice elle-même est, pour les membres AMRAE, téléchargeable, dans la section Commission Systèmes d'Information de l'espace membre de son site web.

Etapes #1 & #2 : description du risque et des impacts (Risques 1 à 5)

	#1 - Risques	#2 - Impacts		
Réf.	**Libellé du risque**	**Impacts assurés**	**Impacts tiers**	**Estimation impact financier (KEUR)**
Explication de la matrice	1. Risque à décrire précisément	2. Impacts à décrire précisément pour vous, assurés, et pour les tiers (exemple : clients)	3. Ces impacts sont-ils couverts par vos polices d'assurance ? (dommages, RC, fraude, rançon et cyber) Préjudice consécutif à cet achat différé Impacts sur les Actifs, le business (CA), les O.L, les 1/3 Lister les types d'impacts, par exemple : Obligations Légales Réclamations 1/3 Perte de CA Valeur des actifs Image de marque Cours de l'action Perte de marché	4, Appréciation de l'impact financier global de la réalisation du risque identifié
R1	Impossibilité d'encaisser des CB dans des magasins (par ex : en raison d'un arrêt des réseaux de télécommunication)	Vente manquée pour le commerçant et perte de la commission pour la banque	Achat différé, préjudice consécutif au non-achat (ex. : solde ou promotion ratée), impossibilité de sortir du parking, …) Perte de CA, reclamations clients.	
R2	Publications d'informations malveillantes ou diffamantes sur un des médias numériques de l'assuré (ex : sites internet, intranet, blogs, Facebook, ...)	Perte d'image et de chiffre d'affaires et/ou baisse de l'action	Si le site est utilisé pour nuire à un tiers : réclamation en RC pour mauvaise surveillance du site; appel au boycott, sanctions pénales Perte de CA, réclamations clients, Image de marque / e-réputation	
R3	Lancement d'attaques contre des entreprises tierces par un pirate qui s'est introduit dans les systèmes de l'assuré	Perte d'image et de chiffre d'affaires et/ou baisse de l'action	Réclamation en RC pour mauvaise surveillance du site; appel au boycott, sanctions pénales Perte de CA, réclamations clients, Image de marque	
R4	Vol d'informations de l'assuré à la suite d'une attaque informatique identifiée telle que la copie de base de données clients de l'assuré par un pirate	Frais de notification, réclamations clients; arrêt d'activité; image de marque; appel au boycott perte de CA concurrence, frais de remplacement des CB	Utilisation frauduleuse de ses données, usurpation d'identité, faux paiements, escroquerie ...	
R5	Copie de données valorisables. Ex : cartes bancaires	Frais de notification, réclamations clients; tentative d'extorsion; image de marque; appel au boycott	Utilisation frauduleuse de ses données, usurpation d'identité	
.../...	.../...	.../...	.../...	.../...

Etapes #1 & #2 : description du risque et des impacts (Risques 6 à 15)

	#1 - Risques	#2 - Impacts		
Réf.	**Libellé du risque**	**Impacts assurés**	**Impacts tiers**	**Estimation impact financier (KEUR)**
Explication de la matrice	1. Risque à décrire précisément	2. Impacts à décrire précisément pour vous, assurés, et pour les tiers (exemple : clients)	3. Ces impacts sont-ils couverts par vos polices d'assurance ? (dommages, RC, fraude, rançon et cyber) Préjudice consécutif à cet achat différé Impacts sur les Actifs, le business (CA), les O.L, les 1/3 Lister les types d'impacts, par exemple : Obligations Légales Réclamations 1/3 Perte de CA Valeur des actifs Image de marque Cours de l'action Perte de marché	4, Appréciation de l'impact financier global de la réalisation du risque identifié
.../...	.../...	.../...	.../...	.../...
R6	Fraude due à la vulnérabilité des SI hébergés et /ou managés par l'infogérant	Perte financière consécutive à la fraude, réclamations, pour lui ou pour ses clients ; image de marque	Utilisation frauduleuse de ses données, usurpation d'identité	
R7	Indisponibilité du SI et du service fourni par l'infogérant à l'assuré suite évènement accidentel sur équipement	Perte financière consécutive à la non fourniture de la prestation, pour lui ou pour ses clients ; image de marque; réclamation de ses clients		
R8	Panne, dérangement (sans dommage matériel) des installations informatiques et/ou des installations d'infrastructures annexes de l'assuré, pouvant entrainer altération ou destruction de données tiers par l'assuré	Perte financière consécutive à la non fourniture de la prestation, pour lui ou pour ses clients ; image de marque; réclamation de ses clients	Hors problème de sous dimensionnement et faute de conception	
R9	Doutes sur la sécurité des données suite à un dommage matériel à l'outil de production chez l'assuré ou chez un prestataire/infogérant	Les données ne sont potentiellement plus fiables et on craint que leur utilisation ne provoque un dommage à l'assuré ou a un tiers. Impacts: coût reconstitution des données, frais supplémentaires, perte temporaire de CA ; image de marque.	Couverture de tous les frais de reconstitutions des données	
R10	Grève, émeute, mouvement populaire générant la destruction des infrastructures de l'assuré, d'un prestataire de service d'hébergement désigné ou infogérant désigné.	Perte financière consécutive à la non fourniture de la prestation, pour lui ou pour ses clients ; image de marque; réclamation de ses clients; dommages matériels	Perte financière consécutive à la non fourniture de la prestation, pour lui ou pour ses clients ; image de marque; réclamation de ses clients ; dommages matériels	
R11	Erreur de l'assuré générant une compromission de la sécurité de données personnelles	Perte financière, pour lui ou pour ses clients ; image de marque; réclamation de ses clients; frais de notification	Utilisation non-souhaitée des données personnelles.	
R12	Erreur de programmation de la part de l'assuré	Perte financière, pour lui ou pour ses clients ; image de marque; réclamation de ses clients		
R13	Défaillance d'une prestation de service technologique (installation d'applicatif, administration de serveurs….) ou défectuosité d'un système développé et opéré par l'assuré pour un client	Image de marque; réclamation de ses clients		
R14	Pénétration dans le système de l'assuré avec destruction des données de l'assuré + données clients, dont des données personnelles	Perte financière, pour lui ou pour ses clients ; image de marque; réclamation de ses clients; frais de notification		
R15	Doutes sur la sécurité des données suite à intrusion dans les systèmes. Coupure/isolation par (décision assuré) du système pour limiter le risque de fraude.	Perte financière consécutive à la non-fourniture de la prestation, pour lui ou pour ses clients ; image de marque; réclamation de ses clients	Association de l'assureur à la prise de décision	
.../...	.../...	.../...	.../...	.../...

Etapes #1 & #2 : description du risque et des impacts (Risques 16 à 20)

	#1 - Risques	#2 - Impacts		
Réf.	**Libellé du risque**	**Impacts assurés**	**Impacts tiers**	**Estimation impact financier (KEUR)**
Explication de la matrice	1. Risque à décrire précisément	2. Impacts à décrire précisément pour vous, assurés, et pour les tiers (exemple : clients)	3. Ces impacts sont-ils couverts par vos polices d'assurance ? (dommages, RC, fraude, rançon et cyber) Préjudice consécutif à cet achat différé Impacts sur les Actifs, le business (CA), les O.L, les 1/3 Lister les types d'impacts, par exemple : Obligations Légales Réclamations 1/3 Perte de CA Valeur des actifs Image de marque Cours de l'action Perte de marché	4, Appréciation de l'impact financier global de la réalisation du risque identifié
R16	Pénétration dans le système de l'assuré avec suspicion de détournement des données assuré + données clients à des fins de fraude.	Ce scenario pose les mêmes interrogations que les R9 et R15, seul le fait générateur change : les données ont été détournées et on craint que leur utilisation ne provoque une dommage à l'assuré ou à un tiers. Coût reconstitution des données, perte temporaire de CA ; image de marque	Acte de malveillance	
R17	Demande de rançon pour éviter une attaque sur le SI			
R18	Virus informatique affectant les systèmes de l'assuré (bombe logique, déni de service)	Perte financière, pour lui ou pour ses clients ; image de marque; réclamation de ses clients; frais de notification		
R19	Déni de service du fait d'un tiers sur le système de l'assuré et son réseau	Perte financière, pour lui ou pour ses clients ; image de marque; réclamation de ses clients; frais de notification		
R20	Utilisation non autorisée des systèmes de l'assuré par des préposés	Perte financière, pour lui ou pour ses clients ; image de marque; réclamation de ses clients; frais de notification		

Etapes #3 & #4 : description des préventions/ protections et traitements par l'assurance (Risques 1 à 7)

	#1 - Risques	#3 - Traitements	#4 - Polices d'assurance				
Réf.	**Libellé du risque**	**Mesures de gestion et de réduction**	**DOMMAGES/PE**	**RC**	**FRAUDE**	**RANCON**	**CYBER**
Explication de la matrice	1. Risque à décrire précisément	5. Décrire les mesures de réductions en place et/ou désirées	6. Quels frais sont couvert par ces polices ? (liste des frais/dépenses couverts) 7. Quels frais ne sont pas couverts par ces polices et lesquels pourriez-vous couvrir en étendant une garantie ? **LEGENDE :** *VERT = GARANTI* *ROUGE = NON GARANTI* *BLEU : Ne Sais Pas – A vérifier*				
R1	Impossibilité d'encaisser des CB dans des magasins (par ex : en raison d'un arrêt des réseaux de télécommunication)		Notamment par : - la garantie malveillance du contrat PE, si arrêt dû à la malveillance - la garantie carence de fournisseur si dommage matériel à l'outil de production du fournisseur	La RC du fournisseur (banque, GIE, fournisseur d'accès) peut être limitée contractuellement; le préjudice lié au non-achat n'est pas direct	Il n'y a pas vol ou détournement des données mais impossibilité de les saisir - exclusion carte bancaire du contrat fraude des banques		Le contrat cyber offre une garantie PE si l'événement est de type Cyber, c'est à dire comportant une atteinte à la sécurité
R2	Publications d'informations malveillantes ou diffamantes sur un des médias numériques de l'assuré (ex : sites internet, intranet, blogs, Facebook, ...)		Garantie malveillance du contrat PE	Garanti si faute professionnelle, frais de décontamination	La malveillance ne porte pas sur un bien assuré		Il semble que le contrat Cyber ne garantisse qu'une attaque aux données existantes et non l'ajout. A négocier.
R3	Lancement d'attaques contre des entreprises tierces par un pirate qui s'est introduit dans les systèmes de l'assuré		Garantie malveillance du contrat PE, bris de machine		La malveillance ne porte pas sur un bien assuré		
R4	Vol d'informations de l'assuré à la suite d'une attaque informatique identifiée telle que la copie de base de données clients de l'assuré par un pirate		Pas de destruction de l'outil de production ni de la donnée qui n'est pas volée au sens pénal du terme.	Garanti si faute de l'assuré gardien des données	La donnée n'est pas volée au sens pénal du terme. A déclarer sur le volet malveillance.		Frais de reconstitution
R5	Copie de données valorisables Ex : cartes bancaires		Pas de destruction de l'outil de production ni de la donnée qui n'est pas volée au sens pénal du terme.	Garanti si faute de l'assuré gardien des données	La donnée n'est pas volée au sens pénal du terme. A déclarer sur le volet malveillance.		Couverture PE limitée
R6	Fraude due à la vulnérabilité des SI hébergés et /ou managés par l'infogérant		La fraude est exclue de la police PE	Garanti si faute de l'assuré gardien des données	Garantie fraude, étendue aux fraudes sur les données de l'assuré situées chez son infogérant		Elle peut couvrir la fraude chez l'infogérant
R7	Indisponibilité du SI et du service fourni par l'infogérant à l'assuré suite évènement accidentel sur équipement		Extension carence de fournisseur de la police PE dû et non dû	Le dommage au tiers n'est pas du à une faute de l'entreprise mais à un événement qui lui est extérieur. Il s'agit donc d'un cas de non-exécution non garanti par l'assurance RC.	Pas de fraude		Garantie défaillance du SI à étendre à l'infogérant.

Etapes #3 & #4 : description des préventions/ protections et traitements par l'assurance (Risques 8 à 15)

	#1 - Risques	#3 - Traitements	#4 - Polices d'assurance				
Réf.	**Libellé du risque**	**Mesures de gestion et de réduction**	**DOMMAGES/PE**	**RC**	**FRAUDE**	**RANCON**	**CYBER**
Explication de la matrice	1. Risque à décrire précisément	5. Décrire les mesures de réductions en place et/ou désirées	6. Quels frais sont couvert par ces polices ? (liste des frais/dépenses couverts) 7. Quels frais ne sont pas couverts par ces polices et lesquels pourriez-vous couvrir en étendant une garantie ? **LEGENDE :** *VERT = GARANTI* *ROUGE = NON GARANTI* *BLEU : Ne Sais Pas – A vérifier*				
R8	Panne, dérangement (sans dommage matériel) des installations informatiques et/ou des installations d'infrastructures annexes de l'assuré, pouvant entrainer altération ou destruction de données tiers par l'assuré		Pas de Dommages matériels dû et pas dû	Le dommage au tiers n'est pas du à une faute de l'entreprise mais à un événement qui lui est extérieur. Il s'agit donc d'un cas de non-exécution non garanti par l'assurance RC.	Pas de fraude		Garantie défaillance du SI
R9	Doutes sur la sécurité des données suite à un dommage matériel à l'outil de production chez l'assuré ou chez un prestataire/infogérant		Frais de recherche de fiabilité des données; frais de reconstitution des données jugées non fiables	Si les données sont à nouveau fiabilisées il n'y aura à priori plus de réclamation du tiers possible.	Pas de fraude		Garantie prestataire
R10	Grève, émeute, mouvement populaire générant la destruction des infrastructures de l'assuré, d'un prestataire de service d'hébergement désigné ou infogérant désigné.		Attention exclusion des grèves et mouvements populaires.	Attention exclusion des grèves et mouvements populaires.	Pas de fraude		Attention exclusion des grèves et mouvements populaires.
R11	Erreur de l'assuré générant une compromission de la sécurité de données personnelles		Pas de dommage à l'outil de production	Garantie si faute de l'assuré	Pas de fraude		Notamment frais de notification
R12	Erreur de programmation de la part de l'assuré		Pas de dommage à l'outil de production	Garantie si faute de l'assuré	Pas de fraude		
R13	Défaillance d'une prestation de service technologique (installation d'applicatif, administration de serveurs….) ou défectuosité d'un système développé et opéré par l'assuré pour un client		Pas de dommage à l'outil de production	Garantie si faute de l'assuré	Pas de fraude		
R14	Pénétration dans le système de l'assuré avec destruction des données de l'assuré + données clients, dont des données personnelles		Garantie malveillance du contrat PE	Garanti si faute de l'assuré	Garantie malveillance du contrat fraude (frais)		
R15	Doutes sur la sécurité des données suite à intrusion dans les systèmes. Coupure/isolation par (décision assuré) du système pour limiter le risque de fraude.		Garantie malveillance du contrat PE. Attention, perte incertaine et éventuel sinistre "intentionnel"	Garanti si faute de l'assuré. Attention, éventuel sinistre "intentionnel"	Garantie malveillance du contrat fraude. Attention, perte incertaine et éventuel sinistre "intentionnel"		
	…/…	…/…	…/…	…/…	…/…	…/…	…/…

Etapes #3 & #4 : description des préventions/ protections et traitements par l'assurance (Risques 16 à 20)

	#1 - Risques	#3 - Traitements	#4 - Polices d'assurance				
Réf.	**Libellé du risque**	**Mesures de gestion et de réduction**	**DOMMAGES/PE**	**RC**	**FRAUDE**	**RANCON**	**CYBER**
Explication de la matrice	1. Risque à décrire précisément	5. Décrire les mesures de réductions en place et/ou désirées	6. Quels frais sont couvert par ces polices ? (liste des frais/dépenses couverts) 7. Quels frais ne sont pas couverts par ces polices et lesquels pourriez-vous couvrir en étendant une garantie ?				
R16	Pénétration dans le système de l'assuré avec suspicion de détournement des données assuré + données clients à des fins de fraude.		Garantie malveillance du contrat PE	Garanti si faute professionnelle	Garantie malveillance du contrat fraude (frais)		
R17	Demande de rançon pour éviter une attaque sur le SI					Garantie à mettre en place	Paiement rançon, frais de négociation
R18	Virus informatique affectant les systèmes de l'assuré (bombe logique, déni de service)		Garantie malveillance du contrat PE	Garanti si faute professionnelle	Garantie malveillance du contrat fraude (frais)		
R19	Déni de service du fait d'un tiers sur le système de l'assuré et son réseau		Garantie malveillance du contrat PE dû et pas dû	Le dommage au tiers n'est pas dû à une faute de l'entreprise mais à un événement qui lui est extérieur. Il s'agit donc d'un cas de non-exécution non garanti par l'assurance RC.	Garantie malveillance du contrat fraude (rais)		
R20	Utilisation non autorisée des systèmes de l'assuré par des préposés		Garantie malveillance du contrat PE	Garanti présomption de faute du fait des préposés.	Garantie malveillance du contrat fraude (frais)		
....	.../...	.../...	.../...	.../...	.../...	.../...	.../...

Etapes #4 : Niveau idéal de garantie et limites actuelles rencontrées (Risques 1 à 7)

	#1 - Risques	#4.1 - Décrire votre niveau de garantie idéal	#4.2 - Limites actuelles / recherchées des Polices d'assurance				
Réf.	**Libellé du risque**	**Description du niveau de garantie idéal**	**DOMMAGES/PE**	**RC**	**FRAUDE**	**RANCON**	**CYBER**
Explication de la matrice	1. Risque à décrire précisément	8. Décrivez votre niveau de garantie idéal	9. Décrivez les limites existantes ou recherchées des polices couvrant votre organisation				
R1	Impossibilité d'encaisser des CB dans des magasins (par ex : en raison d'un arrêt des réseaux de télécommunication)						
R2	Publications d'informations malveillantes ou diffamantes sur un des médias numériques de l'assuré (ex : sites internet, intranet, blogs, Facebook, ...)	Garantie perte d'image. Contrats de gestion de crise					
R3	Lancement d'attaques contre des entreprises tierces par un pirate qui s'est introduit dans les systèmes de l'assuré	Frais de décontamination, frais d'enquête, garantie spéciale Dommages cyber ? Spécial PE sans Dommages ?					
R4	Vol d'informations de l'assuré à la suite d'une attaque informatique identifiée telle que la copie de base de données clients de l'assuré par un pirate	Perte d'exploitation sans dommages (ou avec dommages immatériels)					
R5	Copie de données valorisables Ex : cartes bancaires	Perte d'exploitation sans dommages (ou avec dommages immatériels)					
R6	Fraude due à la vulnérabilité des SI hébergés et /ou managés par l'infogérant						
R7	Indisponibilité du SI et du service fourni par l'infogérant à l'assuré suite évènement accidentel sur équipement						
.../...	.../...	**.../...**	.../...	.../...	.../...	.../...	.../...

Etapes #4 : Niveau idéal de garantie et limites actuelles rencontrées (Risques 8 à 13)

	#1 - Risques	#4.1 - Décrire votre niveau de garantie idéal	#4.2 - Limites actuelles / recherchées des Polices d'assurance				
Réf.	**Libellé du risque**	**Description du niveau de garantie idéal**	**DOMMAGES/PE**	**RC**	**FRAUDE**	**RANCON**	**CYBER**
Explication de la matrice	1. Risque à décrire précisément	8. Décrivez votre niveau de garantie idéal	9. Décrivez les limites existantes ou recherchées des polices couvrant votre organisation				
.../...	.../...	.../...	.../...	.../...	.../...	.../...	.../...
R8	Panne, dérangement (sans dommage matériel) des installations informatiques et/ou des installations d'infrastructures annexes de l'assuré, pouvant entrainer altération ou destruction de données tiers par l'assuré						
R9	Doutes sur la sécurité des données suite à un dommage matériel à l'outil de production chez l'assuré ou chez un prestataire/infogérant						
R10	Grève, émeute, mouvement populaire générant la destruction des infrastructures de l'assuré, d'un prestataire de service d'hébergement désigné ou infogérant désigné.						
R11	Erreur de l'assuré générant une compromission de la sécurité de données personnelles						
R12	Erreur de programmation de la part de l'assuré						
R13	Défaillance d'une prestation de service technologique (installation d'applicatif, administration de serveurs....) ou défectuosité d'un système développé et opéré par l'assuré pour un client						
.../...	.../...	.../...	.../...	.../...	.../...	.../...	.../...

Etapes #4 : Niveau idéal de garantie et limites actuelles rencontrées (Risques 14 a 20)

	#1 - Risques	#4.1 - Décrire votre niveau de garantie idéal	#4.2 - Limites actuelles / recherchées des Polices d'assurance				
Réf.	Libellé du risque	Description du niveau de garantie idéal	DOMMAGES/PE	RC	FRAUDE	RANCON	CYBER
.../...	.../...	.../...	.../...	.../...	.../...	.../...	.../...
R14	Pénétration dans le système de l'assuré avec destruction des données de l'assuré + données clients, dont des données personnelles						
R15	Doutes sur la sécurité des données suite à intrusion dans les systèmes. Coupure/isolation par (décision assuré) du système pour limiter le risque de fraude.	Perte incertaine et éventuel sinistre "intentionnel"					
R16	Pénétration dans le système de l'assuré avec suspicion de détournement des données assuré + données clients à des fins de fraude.						
R17	Demande de rançon pour éviter une attaque sur le SI	Garantie analyse des risques, frais d'enquête, limité en capitaux, quid si échec de la négociation ?					
R18	Virus informatique affectant les systèmes de l'assuré (bombe logique, déni de service)						
R19	Déni de service du fait d'un tiers sur le système de l'assuré et son réseau						
R20	Utilisation non autorisée des systèmes de l'assuré par des préposés						

Annexe 2 : Etat du Marché

Etendue des couvertures en amélioration constante (+30%,)

Les offres des assureurs englobent (quasiment toutes) la combinaison des garanties dommages et RC. La concurrence est forte entre les assureurs "Dommages" et les assureurs "Responsabilité". Amélioration de la cohérence des réponses des assureurs dans les montages en ligne ou en coassurance. Offres de Garanties « Dommages » plus adaptées aux grands risques notamment en Perte d'exploitation et Carence de fournisseurs. Augmentation des plafonds des sous–limites (voire disparition en montage coassurance). On peut constater l'arrivée de nouveaux produits, plus complexes au niveau du texte. Ces couvertures hybrides sont maintenant maitrisées par les assureurs, plusieurs offres combinant assurance (indemnisation) et gestion de crise (service) sont disponibles. Cette couverture peut intervenir en première ligne ou en complément des garanties Dommages ou RC existantes. Certains courtiers ont développé des services connexes en amont pour accompagner les clients sur l'évaluation de ces risques. Apparition de programmes internationaux.

Franchises/Tendances Auto Assurance

Tendance plutôt à la baisse (de 20 à 30 %) compte tenu de la concurrence accrue. Baisse sur les entreprises les moins exposées en termes de taille et de risques. Les assureurs peuvent proposer des franchises moins élevées. Franchise PE exprimée en temps réduite ou convertie en seuil de déclenchement, application d'une franchise unique tous postes garantis. Les garanties gestion de crises sont délivrées sans franchise.

Secteur ne suivant pas la tendance : Distribution

Capacités en hausse

La capacité théorique sur le marché continental est de l'ordre de 355 millions d'euros. Les acteurs de Londres offrent quant à eux 100 millions d'euros supplémentaires. En pratique, les plus grosses capacités placées sur un programme sont plus proches des 100 à 150 millions d'euros.

Tarification compétitive

Très compétitive et plutôt à la baisse compte tenu de la concurrence accrue par l'apparition de nouveaux opérateurs. Environ 20% mais difficile à qualifier en terme de pourcentage (manque de recul, produit trop récent). Baisse sur les entreprises les moins exposées en termes de taille et de risques. Impact de la Réassurance facultative à la hausse sur les tarifications délivrées par les assureurs proposant des apéritions avec des capacités supérieures à 25 millions d'euros. Impact relatif de la sinistralité américaine hors secteur distribution.

www.amrae.fr

Management des Risques et des Assurances de l'Entreprise
80 BOULEVARD HAUSSMANN 75008 PARIS - TEL : +33 (0)1 42 89 33 16 - FAX : +33 (0)1 42 89 33 14 - amrae@amrae.fr - www.amrae.fr