Copyright AMRAE, en partenariat avec le CESIN

MATRICE D'ANALYSE DES RISQUES "CYBER" ET DES COUVERTURES ASSURANCES ASSOCIEES

Légende		
	COUVERT	NON COUVERT
	GARANTIE SOUS CONDITION	JE NE SAIS PAS, JE DOIS VERIFIER
	N/A	

	g	#2 - Impacts			#3 - Traitements	#4 - Polices d'assurance					#4.1 - Décrire votre niveau de garantie idéal	#4.2 - Limites actuelles / recherchées des Polices d'assurance				
Réf.	Libellé du risque	Impacts assurés	Impacts tiers	Estimation impact financier (KEUR)	Mesures de gestion et de réduction	DOMMAGES/PE	RC	FRAUDE	RANCON	CYBER	Description du niveau de garantie idéal	DOMMAGES/PE	RC	FRAUDE	RANCON	CYBER
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.I., 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	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 ?					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)	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, etc. Perte de CA, réclamations clients.			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'évènement 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, ...)	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			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.	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	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			Garantie malveillance du contrat PE, bris de machine		La malveillance ne porte pas sur un bien assuré			Frais de décontamination , frais d'enquête , garantie spéciale Dommages cyber ? Spécial PE sans Dommages ?					
0	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 ...			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	Perte d'exploitation sans dommages (ou avec dommages immatériels)					
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			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	Perte d'exploitation sans dommages (ou avec dommages immatériels)					
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			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	Perte financière consécutive à la non fourniture de la prestation, pour lui ou pour ses clients ; image de marque; réclamation de ses clients				Extension carence de fournisseur de la police PE	Le dommage au tiers n'est pas du à une faute de l'entreprise mais à un évènement 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.						
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			Pas de Dommages matériels	Le dommage au tiers n'est pas du à une faute de l'entreprise mais à un évènement 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	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			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.	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 ;dommages matériels			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	Perte financière, pour lui ou pour ses clients ; image de marque; réclamation de ses clients; frais de notification	Utilisation non-souhaitée des données personelles.			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	Perte financière, pour lui ou pour ses clients ; image de marque; réclamation de ses clients;				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	Image de marque; réclamation de ses clients;				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	Perte financière, pour lui ou pour ses clients ; image de marque; réclamation de ses clients; frais de notification				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.	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			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"			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.	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 a un tiers. Coût reconstitution des données , perte temporaire de CA ; image de marque .	Acte de malveillance			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 a mettre en place	Paiement rançon, frais de négociation	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)	Perte financière, pour lui ou pour ses clients ; image de marque; réclamation de ses clients; frais de notification				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	Perte financière, pour lui ou pour ses clients ; image de marque; réclamation de ses clients; frais de notification				Garantie malveillance du contrat PE	Le dommage au tiers n'est pas du à une faute de l'entreprise mais à un évènement 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 (frais)								
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				Garantie malveillance du contrat PE	Garanti présomption de faute du fait des préposés.	Garantie malveillance du contrat fraude (frais)								
R21	.../...	.../...	.../...	.../...		.../...	.../...	.../...	.../...	.../...	.../...	.../...	.../...	.../...	.../...	.../...
R22																